جامعة التكوين المتواصل
مركز الجزائر شمال- بوزريعة

تقرير تربص لنيل شهادة الدراسات الجامعية التطبيقية
D.E.U.A

الموضوع:
الجريمة المعلوماتية وأثارها الاقتصادية
دراسة حالة: الفيروس المعلوماتي
مركز البحث في الإعلام العلمي والتقني
CERIST

من إعداد الطالبة:	أعضاء اللجنة المناقشة		الأستاذ المشرف:
سوري يسمينة	الأستاذ:	رئيسا	سعيدي صالح
	الأستاذ:	مقررا	الأستاذة المؤطرة:
	الأستاذ:	عضوا	بن صافية حسينة

السنة الدراسية:
٢٠٠٥ ـ ٢٠٠٤

إهـــــــــــــــــــــــــداء

أهدي ثمرة جهدي إلى أعز أم في الوجود، أمي التي كانت سببا في نجاحي و والدي الذي لم يبخل علي بتشجيعه المتواصل، إلى إخوتي محمد و زوجته، عبد الرحمن، رابح و حمزة و أخواتي عائشة وزوجها، صفية ولامية.وأخص بالذكر خولة، رانية، سيد أحمد، سرين هبة و أنيس.

و بصفة خاصة إلى السيد لكحل عقبة و الكتكوت الصغير أكرم و كل الأصدقاء والصديقات: سعاد، سهام، أسية، حنان، سميرة، كريمة و كل الذين لم أذكرهم.

سوري يسمينة

7442559

المقدمة

المقــــــدمـــــة:

شهدت الجريمة قي أشكالها تطورا كبيرا على ما كانت عليه من قبل , حيث كانــت مقتصــرة علــى الأنماط الكلاسيكية كالسرقة و القتل, مما جعل المجتمعات تواجه تحــديات و صــعوبات جديــدة نتيجــة الحركيــة المتصارعة التي شهدها التطور في مختلف الميادين الاقتصادية ,الاجتماعية, و السياسية, فأفرزت هذه الحركة ظواهر جديدة تسعى لاستغلال التطورات الموجودة في النظم القانونية,لتحقيق مكاسب مادية وثراء غير مشروع,بأساليب الغش و الاحتيــــال.وتعد الجرائم الاقتصادية أكثر الجرائم التي عرفت انتشارا واسعا عن غيرها وهي تهدف إلى المساس بالنظام الاقتصادي و المالي للمجتمع , لا سيما تلك التي تنطلق أساسا من المعاملات الالكترونية ذات الطابع الــوطني والدولي, حيث باتت التشريعات الوطنية بمفردها عاجزة عن التصدي لها بحلول منعزلة حيث يطفو تنازع الاختصاص التشريعي و القضائي, و محاولة التعرف على القانون الواجب التطبيق و القضاء المختص , لدا ظهرت الحاجة إلــى ميلاد قواعد قانونية ذات طابع دولي، ذلك أن دولية العلاقات القانونية تقتضي دولية القواعد القانونية التي تحكمها.

و يمكن القول بأنها جرائم حديثة وجدت على اثر التطور الاقتصادي و الاجتماعي و التكنولوجي للمجتمــع، فتعتبــر الجريمة المعلوماتية في مجال برامج الحاسوب الآلي و مدى تأثيرها على المجال الاقتصادي من القضايا الشائكة فــي عالمنا اليوم, لدرجة أنها أصبحت تشكل خطرا على العلاقات و المؤسسات العمومية والخاصة,وهذا نظــرا للخســائر المادية الكبرى الناجمة عن ذلك و التي تقدر بملايين بل بملايير الدولارات عبر أنحاء العالم.

1. الاشكالية:

جاءت اشكالية البحث وفق مجموعة من التساؤلات نوردها على النحو التالي:

- ما هي مقومات الجريمة المعلوماتية؟
- ما هو مفهوم الجريمة المعلوماتية؟
- عل أي أساس يضبط مرتكبي الجريمة المعلوماتية؟
- كيف يمكن تكييف الجريمة المعلوماتية قانونا؟
- ما هي أساليب الإختراق ومدى تأثيرها على الجانب الاقتصادي؟
- ما هي أساليب مكافحة الجريمة المعلوماتية؟

2. الفرضيات:

و على ضوء هذه الإشكاليات، رأينا صياغة بعض الفرضيات لكي تكون أكثر تحديدا و ضبطا لإشكالية البحث و هي كالتالي:

- وضع التشريعات جديدة عن طريق التنسيق على الأقل مع بعض الدول على المستوى العالمي وإبرام اتفاقيات أمر من شأنها أن تقلل من مخاطر الجريمة المعلوماتية.
- ردع محاولات الاختراق والتجسس على شبكة المعلوماتية ، مرهونا بدراسة مواطن الضعف في المنظومة القانونية ز سد الثغرات القانونية.
- ضرورة وجود إدارة تعمل على مراقبة الشبكة المعلوماتية تتمتع بخبرة وكفاءة و أساليب و إمكانيات متطورة لموجهة ظاهرة الجريمة المعلوماتية و اختراق الحواسب عبر شبكة الأنترنيت.

3. دوافع الاختيار :

ارتأينا اختيار هذا الموضوع وذلك لأمرين:

أولا: أن الجريمة المعلوماتية تأخذ طابع قانوني وذلك باعتبارها سلوك منافٍ للقواعد و النصوص القانونية و بالتالي إمكانية دراستها من هذا الجانب و معرفة مقومات هذه الجريمة و كيفية تكييفها و تدرجها في سلم العقوبات المقررة.

ثانيا : باعتبار الجريمة المعلوماتية موضوعا أو واقعة تمسّ اقتصاد الدولة، خاصة إذا ما عرف نشاطه تأثيرا وتغلغلا في الحياة الاقتصادية و ما تمثله من إهدار لمصالح العمومية و الخاصة أمام تزايد عمليات الاختراق و التجسّس و التخريب و سرقة المعلومات و اتساع شبكة الانترنيت.

4.الأهداف :

هدفنا من وراء البحث الإطلاع على الجريمة المعلوماتية من جميع جوانبها القانونية وعلاقتها بالجانب الإقتصادي و دوافع ارتكابها و دوافع الشروع في مشروع قانون من خلال فرض العقوبات و التدابير و غيرها من الإجراءات الكفيلة بالحد من خطورة الجريمة و ما يترتب عليها من أثار إقتصادية و الوقوف أمام تزايد و تفاقم هده المشكلة.

5.المنهج المتبع :

نظرا لطبيعة الموضوع في ظل غياب المراجع اعتمدنا المنهج الوصفي لأجل التعريف بالظاهرة محل البحث، محاولين الوقوف على مخاطر و سلبيات الظاهرة على البنية الإقتصادية مما فرض علينا كذلك اتباع منهج إستنتاجي من أجل الخروج بنتائج اختيار الفرضيات موضوع المقدمة.

6.محاور دراسة البحث :

جاء موضوع دراستنا في فصلين و ذلك وفقا للخطة التالية:

الخطـــــــة :

المقدمـــة

- **الفصل الأول: "ماهية الجريمة المعلوماتية"**

المبحث الأول: تعريف الجريمة المعلوماتية و تصنيفها

المطلب الأول: تعريف الجريمة المعلوماتية

المطلب الثاني: طبيعة الجريمة المعلوماتية

المبحث الثاني:دورالكمبيوتر في الجريمة المعلوماتية وأسس تصنيفها

المطلب الأول: دور الكمبيوتر في الجريمة

المطلب الثاني: تصنيف جرائم المعلوماتية

- **الفصل الثاني: "ميكانزمات ودوافع ارتكاب الجريمة المعلوماتية"**

المبحث الأول: مرتكبي الجرائم المعلوماتية

المطلب الأول: صفات مرتكبي الجريمة المعلوماتية

المطلب الثاني: دوافع ارتكاب الجريمة المعلوماتية

المبحث الثاني: السمات المميزة للجرائم المعلوماتية ووسائل الحماية

المطلب الأول:السمات المميزة للجرائم المعلوماتية عن غيرها من الجرائم

المطلب الثاني: وسائل الحماية من الجريمة المعلوماتية

الخاتمة

الفصل الأول

ماهية الجريمة المعلوماتية

الفصل الأول : " ما هية الجريمة المعلوماتية"

إن موضوع الجريمة المعلوماتية يعتبر بحد ذاته موضوع الساعة و مشكل كل الدول عامـــة ولا سيما في الجزائر, و تزداد أهمية تلك المسألة أمام الطابع الدولي و العالمي لشبكة الأنترنت, فهـــذه الأخيرة تعتبر سلاح ذو حدين, يعمل بين جنبيه الظلمة و النور يعكس وجهي الخير و الشرفي الانسان، فهو وسيلة للربط و الاتصال و التقارب و تبادل المعلومات و المنافع بين أفراد بني الانســـان, الا أنـــه يمكن أن يكون أداة تزوير و كذب و تضليل و بث الرذيلة و التعدي على حقوق الآخرين. لذا ظهـــرت الحاجة الماسة في الحد من هذا الجانب المظلم, و ما ينجم عنه من خسائر اقتصادية.

و من خلال هذا الفصل سنحاول استعراض الجريمة المعلوماتية, وذلك من خلال تعريفها , تصـــنيفها، تحديد موضوعها و خصائصها و كذا أركانها و طبيعتها القانونية.

المبحث الأول: " تعريف الجريمة المعلوماتية و تصنيفها"

لقد نمت الانترنت بشكل مذهل خلال السنوات العشر الأخيرة, فبعد أن كانت مجرد شبكة أكاديمية صغيرة أصبحت تضم الآن ملايين المستخدمين في كافة المدن حول العالم و تحولت من مجرد شبكة بحث أكاديمي الى بيئة متكاملة للاستثماروالعمل و الانتاج والاعلام والحصول علىالمعلومات من جهة ,ومسرح للجريمة من جهة أخرى, ففي البداية لم يكن ثمة اهتمام بمسائل الأمن بقدرما كان الاهتمام ببناء الشبكة و توسيع نشاطها , ولهذا لم يتم بناء الشبكة في المراحل الأولى على نحو يراعي تحديات أمن المعلومات فالاهتمام الأساسي تركز على الربط والدخول و لم يكن الأمن من بين الموضوعات الهامة في بناء الشبكة. وهذا مأدى الى التعدي على هذه الشبكة و الموجهة ضد مكونات النظام المعلوماتي.

المطـــــــلب الأول : " تعريف الجريمة المعلوماتية"

ثمة تباين كبير بشأن الاصطلاحات المستخدمة للدلالة على الظاهرة الجرمية الناشئة في بيئة الكمبيوتر وفيما بعد بيئة الشبكات, وهو تباين رافق مسيرة نشأة و تطور ظاهرة الاجرام المرتبط أو المتصل بتقنية المعلومات فابتداءا من اصطلاح اساءة استخدام الكمبيوتر, مرورا باصطلاح احتيال الكمبيوتر, الجريمة المعلوماتية اصطلاحات جرائم الكومبيوتر, و الجريمة المرتبطة بالكمبيوتر،جرائم التقنية العالية و غيرها الى جرائم الهاكرز أو الاختراقات فجرائم الكمبيوتر و الأنترنات و أخيرالسيبر كرايم .

الفرع الأول : " التعريفات المختلفة للجريمة المعلوماتية القائمة على معيار قانوني"

هي جريمة تطال المعرفة, الاستخدام, الثقة, الأمن, الربح و المال, السمعة, الاعتبار, و مع كل هذا فهي لا تطال حقيقة غير المعلومات, لكن المعلومات بأشكالها المتباينة في البيئة الرقمية تصبح شيئا فشيئا المعرفة و وسيلة الاستخدام و هدفه.

أولا : " المقصود بالجريمة المعلوماتية"

تعرف الجريمة عموما, في نطاق القانون الجنائي, الذي يطلق عليه أيضا تسميات قانون الجزاء و قانون العقوبات بأنها "فعل غير مشروع صادر عن ارادة جنائية يقرر له القانون عقوبة أوتدبير احترازيا"**1** " وعلى الرغم من التباين الكبيرفي تعريفات الجريمة بين الفقهاء القانونيين و بينهم و بين علماء الاجتماع الا أننا تخيرنا هذا التعريف استثنادا الى أنه التعريف الكامل كما يرى الفقه, فهو ما حدد عناصر الجريمة إلى جانب بيانه لأثرها."**2**" و تكمن أهمية هذه القاعدة في تعريف الجريمة, في بيان عناصرالجريمة السلوك و السلوك غير المشروع وفق القانون, الادارة الجنائية و أثرها, العقوبة أو التدابير التي يفرضها القانون من شأنه في الحقيقة أن يعطي تعريفا دقيقا لوصف الجريمة عموما و يميز بينها و بين الأفعال في نطاق الأخلاق, أو الجرائم المدنية أو الجريمة المعلوماتية.

1- محمود نجيب حسني, شرح قانون العقوبات- القسم العام- الطبعة السادسة - دار النهضة العربية- القاهرة1989ص 40.
2- محمود حسني- نفس المرجع- ص40.

ثانيا : " التعريفات القائمة على موضوع الجريمة"

من التعريفات التي تستند إلى موضوع الجريمة, أو أحيانا الى أنماط السلوك محل التجريم, تعريفها بأنها " نشاط غير مشروع موجه لنسخ او تغيير أو حذف أو الوصول الى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقة"**1**". كما تعرف كذلك:" كل سلوك غيرمشروع او غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"**2**".

" أي نمط من هذه الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات"**3**".

" هي الجريمة الناجمة عن ادخال بيانات مزورة في الأنظمة و اساءة استخدام المخرجات اضافة الى أفعال أخرى تشكل جرائم أكثرتعقيدا من الناحية التقنية, مثل تعديل الكمبيوتر."**4**"

و ما من شك أن معيار موضوع الجريمة كأساس للتعريف يعد من أهم المعايير و أكثرها قدرة على ايضاح طبيعة و مفهوم الجريمة محل التعريف.

الا أن هذه التعريفات لا تستند في الحقيقة على موضوع الجريمة بالمعنى القانوني الذي هو محل الاعتداء.

ثالثا : " التعريفات القائمة على وسيلة ارتكاب الجريمة "

ان أصحابها ينطلقون من ان الجريمة المعلوماتية تتحقق باستخدام الكمبيوتر كوسيلة لارتكاب الجريمة , من هذه التعريفات :

" فعل اجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية "**5**"

" كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب" تعريف تاديمان.

1- تعريف الأستاذ روزن بلات، ص31, مشار اليه لدى الدكتور رستم.

2- تعريف هدى قشقوش, جرائم الحاسب الالكتروني ,الطبعة الاولى,دار النهضة العربية - القاهرة- 1992- ص20.

3- تعريف آرثر سولارز, مشار اليه لدى الدكتور رستم ص31.

4- واحد من عدة تعريفات وضعها مكتب المحاسبة العامة للو.م.أ- أنظر www.Goa.gov.

5 - Tom forester, essential problems to hig- tech society first MTT pres edition Cambridge massachusetts, 1989, p 104

هي الجريمة التي تلعب فيها البيانات الكمبيوترية و البرامج المعلوماتية دورا رئيسيا"**1**"

ان تعريف الجريمة لا يستدعي فقط الوسائل المستخدمة لتحقيقه فحسب بل الرجوع الى العمل الأساسي المكون لها , فالجريمة توجه للمعلومات أساسا, و هي قد تكون مجردة من تجسيد أية قيمة مالية و قد تجسد فى الحقيقة اموالا.

<u>الفرع الثاني</u> : " التعريفات القائمة على أساس شخصي"

فقد وضعت عدة تعريفات التي تقوم على أساس سمات شخصية لدى مرتكب الفعل , و هي تحديدا سمة الدراية و المعرفة التقنية.

من هذه التعريفات, تعريف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث و تبنتها الوزارة في دليلها لعام 1979, حيث عرفت بأنها "آلة جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها " و من هذه التعريفات أيضا تعريف دافيد طوبسن بأنها "أية جريمة يكون متطلبا لافترضها أن تتوفر لدى فاعلها معرفة بتقنية الحاسب" و تعريف ستين شاكلر بأنها "أي فعل غير مشروع تكون المعرفة بتقنية الكمبيوتر أساسية لارتكابه والتحقيق فيه و ملاحقته قضائيا"**2**"

<u>الفرع الثالث</u> : " التعريفات التي تعتمد على معايير عدة"

ان شرط المعرفة التقنية, شرط شخصي متصل بالفاعل غير أن هذه الجرائم يرتكب جزء كبير منها من قبل مجموعة تتوزع أدوارهم بين التخطيط و التنفيذ و التعريض و المساهمة, و قد لا تتوفر لدى بعضهم المعرفة بتقنية المعلومات, ثم ماهي حدود المعرفة التقنية, و ما هو معيار و جودها للقول بقيام الجريمة؟

1- تعريف مكتب تقييم التقنية بالولايات م.أ- د. رستم سابق ص 29 و 30 .
2- أنظر د. رستم سابق ص 32.

إن التطور الذي شهدته وسائل التقنية نفسها أظهرت الاتجاه نحو تبسيط وسائل المعالجة و تبادل المعطيات

و تحويل الأجهزة المعقدة فيما سبق إلى أجهزة سهلة الاستخدام حتى ممن لا يعرف شيئا في علوم الكمبيوتر, ولم يعد مطلوبا العلم والمعرفة العميقين ليتمكن شخص من إرسال آلاف رسائل البريد الالكتروني دفعة واحدة الى أحد المواقع لتعطيل عملها, كما لم يعد صعبا أن يضمن أي شخص رسالة بريدية فيروسا التقطه كبرنامج عبر الانترنت أو من خلال صديق فيبثه للغير دون أن يكون عالما أصلا بشيء مما يتطلبه بناء مثل هذه البرامج الشريرة.

و هناك من التعريفات من يعتمد معايير عدة لبيان ماهية الجريمة المعلوماتية, من هذه التعريفات ما يقرره الأستاذ جون كار ول من أن الجريمة المعلوماتية هي "أي عمل ليس له في القانون أو أعراف قطاع الأعمال جزاء, يضر بالأشخاص أو الأموال, ويوجه ضد أو يستخدم التقنية المتقدمة(العالية) لنظم المعلومات"**1**" فهو يعتمد معايير عدة:

<u>أولها:</u> عدم وجود جزاء لمثل هذه الأفعال, رغم توافر جزاءات خاصة لبعض هذه الجرائم في العديد من التشريعات.

<u>ثانيها:</u> تحقيق الضرر للأشخاص أو الأموال.

<u>ثالثها:</u> توجه الفعل ضد أو استخدام التقنية المتقدمة لنظم المعلومات

بأنها :" واقعة تتضمن تقنية الحاسب و مجني عليه يتكبد أو "sheldon-j.Hecht" كما يعرفها الأستاذ يمكن أن يتكبد خسارة وفاعل يحصل على عن عمد أو يمكنه الحصول على مكسب"

و الذي يرى بأنها : Fighting Computer في مؤلفه Donn.B.Parker و تعريف الفقيه

" أي فعل متعمد مرتبط بأي وجه بالحسابات, يتسبب في تكبد أو إمكانية تكبد مجني عليه لخسارة أو حصول أو إمكانية حصول مرتكب على مكسب "

و يستخدم للدلالة على جريمة التعبير "إساءة استخدام الحاسوب".

1- أنظر د.رستم سابق ص 33.

كما عرفها خبراء متخصصون من بلجيكا في معرض ردهم على استبيان منظمة التعاون الاقتصادي التنمية O E C D بأنها:" كل فعل أو امتناع من شأنه الاعتداء على الأمواج المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية" "**1**"

و هذا التعريف متبنى من قبل العديد من الفقهاء و الدارسين. "**2**" بوصفه لديهم أفضل التعريفات لأن هذا التعريف واسع يتيح الاحاطة الشاملة قدر الامكان بظاهرة جرائم المعلوماتية و لأنه يتيح امكانية التعامل مع التطورات المستقبلية التقنية.

المطلب الثاني : " طبيعة الجريمة المعلوماتية "

ان الاعتداء على كيانات الأجهزة التقنية المادية يتعدد وصفها و مهامها من الوجهة التقنية ,ويخرج من نطاق جرائم الكمبيوتر لترتد إلى موقعها الطبيعي , و هي الجرائم التقليدية ,باعتبار هذه الماديات مجسدة لمال منقول مادي تنهض به قواعد و مبادىء و نصوص القانون الجنائي ,و اذا كان من وجوب الحديث عن الاعتداءات على الكيانات المادية في نطاق ظاهرة جرائم الكمبيوتر و الأنترنت ,فانه متعلق فقط بقيمتها الاستراتيجية كمخازن للمعلومات و أدوات لمعالجتها و تبادلها مما يستدعي نقاش تطوير أليات حمايتها خاصة من أنشطة الارهاب و التخريب المعادية للتقنية,و لكن في نطاق النصوص التقليدية لا في نطاق ظاهرة جرائم الكمبيوتر المستجدة ,مع التنبيه الى أن أفعال الاتلاف والتدمير المرتكبة في نطاق جرائم الكمبيوتر و الأنترنات هي الموجهة للنظم و المعطيات و ليس لماديات الأجهزة.

1- WWW.OECD.ORG

2- د. رستم, السابق ص 35.

الفرع الأول : " تاريخ تطور الجريمة المعلوماتية "

إن مفهوم الجريمة المعلوماتية مرتبط بتطور تاريخي تبعا لتطور التقنية واستخداماتها، ففي المرحلة الأولى من شيوع استخدام الكمبيوتر في الستينات اقتصرت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر وترا فقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم بالمعنى القانوني أم ظاهرة جرمية مستجدة بآثار الجدل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في بيئة أو مهنة المعلوماتية. ومع تزايد استخدام الحواسب الشخصية في منتصف السبعينيات ظهرت عدد من الدراسات القانونية التي اهتمت بجرائم المعلوماتية وعالجت عدد من قضايا الجرائم الفعلية, و في الثمانينات طفا على السطح مفهوم جديد لجرائم المعلوماتية ارتبط بعمليات اقتحام نظم الكمبيوتر عن بعد و أنشطة نشر و زراعة الفيروسات المعلوماتية التي تقوم بعمليات تدميرية للملفات أو البرامج من طرف المخترفين للأنظمة المعلوماتية,القادرين على ارتكاب أفعال تستهدف الاستيلاء على المال أو تستهدف التجسس أو الاستيلاء على البيانات السرية الاقتصادية والاجتماعية والسياسية والعسكرية.

وشهدت التسعينيات نمو هائلا من حقل الجرائم التقنية وتغييرا في نطاقها ومفهومها, وكان ذلك بفعل ما أحدثته شبكة الانترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكات المعلومات, وأكثر ما مورست ضد مواقع الانترنت التسويقية الناشطة والهامة التي يعني انقطاعها عن الخدمة لساعات خسائر مالية بالملايين إن لم تكن بالملايير.

وفي نفس الفترة إلى يومنا الحالي نشطت جرائم نشر الفيروسات عبر مواقع الانترنت لما تسهله من انتقالها إلى ملايين المستخدمين في ذات الوقت, وظهرت أنشطة الرسائل والمواد الكتابية المنشورة على الانترنت أو المرسلة عبر البريد الكتروني المنطوية علىاثارة الأحقاد أو المســاس بكرامــة و اعتبــار الأشــخاص أو المستهدفة الترويج لمواد أو أفعال غير قانونية وغير مشرعة.

الفرع الثاني : "موضوع الجريمة المعلوماتية"

إن محل الجريمة المعلوماتية هو دائما المعطيات إما بذاتها أو بما تمثله هذه المعطيات التي قد تكون مخزنة داخل النظام أوعلى أحد وسائط التخزين أو تكون طور التبادل ضمن وسائل الاتصال المندمجة مع نظام الحوسبة. فان كل جرم يمس مصلحة يقدر المشرع أهميته و أهمية التدخل لحمايتها، و المصلحة محل الحماية في ميدان جرائم المعلوماتية هي الحق في المعلومات كعنصر معنوي ذي قيمة اقتصادية عالية، ويشمل ذلك الحق في الوصول إلى المعلومات و انسيابها وتدفقها وتبادلها و تنظيم استخدامها كل ذلك على نحو مشروع ودون مساس بحقوق الآخرين في المعلومات.

المبحث الثاني : " دور الكمبيوتر في الجريمة المعلوماتية وأسس تصنيفها "

ترتكب الجريمة المعلوماتية باستخدام الحاسوب أو النظام المعلوماتي كوسيلة للاعتداء أو أداة لتنفيذها وهي كظاهرة إجرامية جديدة لها ما يميزها عن غيرها من الجرائم التقليدية من خصائص متعلقة بها وحدها دون سواها من الجرائم الأخرى وقد سعى الفقهاء الدارسون لها إلى تحديد دور الكمبيــوتر فــي الجريمــة وأسس تصنيفها وهذا ما سوف نتعرض له بالتفصيل في هذا المبحث.

المطلب الأول : " دور الكمبيوتر في الجريمة"

إن دور الكمبيوتر في الجريمة متعدد، فهو إما أن يكون الهدف المباشر للاعتداء أو هو وسيلة الاعتداء لتحقيق نتيجة جرمية لا تتصل مباشرة بالمعطيات وإنما تمثله أو تجسده أو هو بيئة أو مخزن للجريمة، و يجب أن لا يوقعها أي من هذه الأدوار في أي خلط بشان محل الجريمة أو وسيلة ارتكابها. فان محل الجريمة دائما هو المعطيات ووسيلة ارتكاب الجريمة المعلوماتية هو أداة ارتكاب الجريمة."**1**"

الفرع الأول: " أدوار الكمبيوتر في ميدان ارتكاب الجرائم"

يلعب الكمبيوتر ثلاث أدوار في ميدان ارتكاب الجرائم في حقل اكتشافها، يكون للمخترق الدور الرئيسي في ارتكابها:

أولا : " الكمبيوتر هدف للجريمة"

قد يكون الكمبيوتر هدف للجريمة (Target of an offense)، و ذلك كما في حالة الدخول غير المصرح به إلى النظام أو زراعة الفيروسات لتدمير المعطيات والملفات المخزنة أوتعديلها، و كما في حالة الاستيلاء على البيانات المخزنة أو المنقولة عبر النظم.

ومن أوضح المظاهر لاعتبار الكمبيوتر هدفا للجريمة في حقل التصرفات غير القانونية عندما تكون السرية (Confidentiality) وتكون هجمات الكمبيوتر موجهة إلى المعلومات التي يحملها أو الخدمات بقصد المساس بالسرية أو المساس بالمحتوى و السلامة، أو تعطيل القدرة أو الكفاءة و هدف هذا النمط

1- د.رستم، السابق ص 35.

الإجرامي هو نظام الكمبيوتر و بشكل خاص المعلومات المخزنة داخله بهدف السيطرة على النظام دون أن يدفع الشخص مقابل للاستخدام (سرقة خدمات الكمبيوتر, أو وقت الكمبيوتر). توصف بشكل شائع في هـده الأيام بأنشطة الهاكرز كناية عن فعل الاختراق (Hacking).

ثانيا : " الكمبيوتر أداة الجريمة "

كما في حالة استغلال الكمبيوتر للاستيلاء على أموال بإجراء تحويلات غير مشرعة أو استخدام التقنية في عمليات التزييف و التزوير، أو استخدام التقنية في الاستيلاء على أرقام بطاقات ائتمان و إعادة استخدامها والاستيلاء على الأموال بواسطة ذلك، حتى أن الكمبيوتر كوسيلة قد يستخدم في جرائم القتل، كما في الدخول إلى قواعد البيانات الصحية والعلاجية الإلكترونية للتأثير على عمل برمجيات التحكم في الطائرة أو السفينة بشكل يؤدي إلى تدميرها قتل ركابها.

ثالثا : " الكمبيوتر بيئة الجريمة"

وقد يكون الكمبيوتر بيئة الجريمة، و ذلك كما في تخزين البرامج المقرصنة فيه أو في حالة استخدام لنشر المواد غير القانونية أو استخدامه كأداة تخزين أو اتصال لصفقات ترويج المخدرات وأنشطة أخرى غير مشروعة.

وطبعا يمكن للكمبيوتر أن يلعب الأدوار الثلاثة معا، ومثال ذلك أن يستخدم أحد مخترقي الكمبيوتر جهازه للتوصل دون تصريح إلى نظام مزود خدمات انترنت (مثال نظام شركة أمريكا أون لاين on ligne) ومن ثم يستخدم الدخول غير القانوني لتوزيع برنامج مخزن في نظامه (أي نظام المخترق) فهو قد ارتكب فعلا موجها نحو الكمبيوتر بوصفه هدفا (الدخول غير المصرح به) ثم استخدم الكمبيوتر لنشاط جرمي تقليدي (عرض و توزيع المصنفات المقرصنة) و استخدام كمبيوتره كبيئة أو مخزن للجريمة عندما قام بتوزيع برنامج مخزن في نظامه.

الفرع الثاني : " دور الكمبيوتر في اكتشاف الجريمة"

إن الكمبيوتر يستخدم الآن على نطاق واسع في التحقيق الاستدلالي لكافة الجرائم، عوضا عن أن جهات تنفيذ القانون تعتمد على النظم التقنية في إدارة المهام من خلال بناء قواعد البيانات ضمن جهاز إدارة العدالة و التطبيق القانوني، و مع تزايد نطاق جرائم المعلوماتية و اعتماد مرتكبيها على وسائل التقنية المتجددة والمتطورة فانه أصبح لزاما استخدام نفس و سائل الجريمة المتطورة للكشف عنها، من هنا يلعب الكمبيوتر ذاته دورا رئيسيا في كشف جرائم المعلوماتية و تتبع فاعليها بل و إبطال أثر الهجمات التدميرية لمخترقي النظم و تحديدا هجمات الفايروسات و قرصنة البرمجيات.

الفرع الثالث : " محل الجريمة المعلوماتية "

تمثل الجرائم المعلوماتية طائفة الجرائم المنصبة على المعلومات بمفهومها الواسع (بيانات, معلومات, برامج تطبيقية و برامج تشغيل), أما بالنسبة للمكونات المادية للحاسوب فالموقف الغالب يتجه إلى اعتبارها من قبيل الجرائم الواقعة عليها مما يندرج في نطاق الجرائم التقليدية حتى تلك التي تستهدف نظام الحاسوب باعتباره المعبر عن عصر التقنية, فهي تستهدف المال باعتبار مكونات الحاسوب المادية أموالا منقولة تصلح محلا للاعتداء عليها بالجرائم الموصوفة بوقوعها على المال, وبجرائم الإتلاف و التخريب."1"
فان محل الجريمة المعلوماتية دائما معطيات الحاسوب, و تستهدف هذه الجرائم الحق في المعلومات, و يمتد تعبير الحق في المعلومات يشمل الحق في انسيابها و تدفقها أو بما تمثله من أموال أو أسرار أو بيانات شخصية سواء كانت مدخلة, معالجة, مخزنة و منقولة.

1- WWW.GOCSI.COM

فاختراق أحدهم مثلا لنظام الحاسوب لأحد البنوك و التلاعب في البيانات (المجسدة) بغرض الاستيلاء على المال يعتبر جرم في حد ذاته و سرقة المال.

و نعطي مثال آخر, إذ في حالة اختراق شخص لشبكة المعلومات بتجاوز إجراءات الأمن مستخدما كلمة السر مثلا أو كلمة المرور (Pass Word), و استخدم النظام الذي اخترقه دون تصريح أو إذن مسبق ودون مقابل ولم يحدث ضرر للنظام ذاته، و لم يستولي على المعلومات السرية المخزنة داخل النظام, فهنا يعتبر استخدامه هذا غير مشروع, ففي حالة ما إذا استولى على المعلومات السرية المتصلة مثلا بالحياة الخاصة (بيانات شخصية), ففي كل الحالات تعتبر المعلومات محل الجريمة المعلوماتية سواء كانت تمثل بيانات أو أموال أو معطيات السرية.

إن الأفعال التي تعبر عن الجرائم المعلوماتية يفترض أن تؤسس على أن المصلحة التي يحميها القانون هي الحق في المعلومات و على أن موضوع الجريمة المعلوماتية و محل الاعتداء المباشر هو المعطيات, والحاسوب يلعب دور الأداة في الاعتداء, فيكون النظام الموجود فيه هدفا للجريمة.

المطلب الثاني : " تصنيف جرائم المعلوماتية "

يصنف الفقهاء و الدارسون جرائم المعلوماتية ضمن فئات متعددة, تختلف حسب الأساس والمعيار الذي يستند إليه, فبعضهم يقسمها إلى جرائم ترتكب على نظم الحاسوب و أخرى ترتكب بواسطته و بعضهم يصنفها ضمن فئات بالاستناد إلى الأسلوب المتبع في الجريمة و غيرهم يؤسس تقسيمه على تعدد محل الاعتداء, و التي تقع على الأموال أو الحياة الخاصة.

سنحاول أن نقف على أبرز التصنيفات بالاحاطة بمختلف الأنماط التي ستكون محل دراسة في هذا الفصل.

الفرع الأول : " تصنيف الجرائم تبعا لنوع المعطيات و محل الجريمة "

و تشمل كل من الجرائم الماسة بقيمة معطيات الحاسوب و كل ما يحمله من معلومات هامة, سرية, و الجرائم الماسة بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة,و الجرائم الماسة بحقوق الملكية الفكرية لبرنامج الحاسوب و نظمه (جرائم قرصنة البرمجيات), الناتجة عن اتساع شبكة الانترنت و ازدياد عدد المستخدمين لها عبر العالم.

أولا: **" الجرائم الماسة بقيمة معطيات الحاسوب "**

و تشمل هذه الطائفة فئتين:

أولهما: الجرائم الواقعة على ذات المعطيات كجرائم الإتلاف و التشويه للبيانات و المعلومات و برامج الحاسوب بما في ذلك استخدام وسيلة (الفيروسات المعلوماتية)

و ثانيها: الجرائم الواقعة على ما تمثله المعطيات آليا, من أموال أو أصول, كجرائم غش الحاسوب التي تستهدف الحصول على المال أو جرائم التجارة بالمعطيات و جرائم التلاعب في المعطيات المخزنة داخل نظم الحاسوب و استخدامها (كتزوير المستندات المعالجة آليا و استخدمها).

ثانيا : " الجرائم الماسة بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة "

و تشمل جرائم الاعتداء على المعطيات السرية المخزنة داخل نظم الحاسوب أو المحمية و جرائم الاعتداء على البيانات الشخصية المتصلة بالحياة الخاصة.

ثالثا : " الجرائم الماسة بحقوق الملكية الفكرية لبرنامج الحاسوب و نظمه "

(جرائم قرصنة البرمجيات)

التي تشمل نسخ و تقليد البرامج و إعادة إنتاجها و صنعها دون ترخيص و الاعتداء على العلامة التجارية و براءة الاختراع.

الفرع الثاني : " تصنيف الجرائم تبعا لدور الكمبيوتر في الجريمة "

عرضنا فيما تقدم لدور الكمبيوتر في الجريمة, فقد يكون كهدف الاعتداء, و قد يكون وسيلة ارتكاب الجريمة في إطار مفهوم (الجرائم المرتبطة بالكمبيوتر), كما قد يكون الكمبيوتر وسيلة ارتكاب الجريمة أو وسطها أو مخزن للمادة الجرمية, و يقصد بها تخزين المواد الجرمية أو المستخدمة في ارتكاب الجريمة أو الناشئة عنها.

لقد أوجد مشروع الاتفاقية الأوروبية."1" تقسيما جديدا نسبيا, فقد تضمن أربع طوائف رئيسية لجرائم المعلوماتية و الانترنت:

1- الجرائم التي تستهدف عناصر (السرية و السلامة):

* الدخول غير القانوني (غير المصرح به)

* الاعتراض غير القانوني.

* تدمير المعطيات.

* اعتراض النظم.

* إساءة استخدام الأجهزة.ذ

1-اتفاقية أوروبية سنة 2001 لمكافحة الجرائم المعلوماتية, و هو جهد تقوده دول أوربا بتدخل و مساهمة كل من أستراليا, كندا و الولايات المتحدة الأمريكية.

2- الجرائم المرتبطة بالكمبيوتر :

* التزوير المرتبط بالكمبيوتر.

* الاحتيال المرتبط بالكمبيوتر.

3- الجرائم المرتبطة بالمحتوى, و تنظم طائفة واحدة وفق هذه الاتفاقية و هي الجرائم المتعلقة بالأفعال الإباحية و لا أخلاقية.

4- الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة- قرصنة البرمجيات.

الفرع الثالث : " تصنيف الجرائم تبعا لمساسها بالأشخاص و الأموال "

نجد هذا التصنيف شائعا في الدراسات و الأبحاث الأمريكية, و كذا التقسيم الذي تضمنه مشروع القانون النموذجي لجرائم المعلوماتية و الانترنت."1"

و في نطاقه تم تقسيم جرائم المعلوماتية و الانترنت إلى: الجرائم الواقعة على الأشخاص و الجرائم الواقعة على الأموال عدا السرقة, و جرائم السرقة والاحتيال, جرائم التزوير و جرائم المقامرة, جرائم ضد الآداب و جرائم ضد المصالح الحكومية, و يلاحظ أن التقسيم يقوم على فكرة الغرض النهائي أو المحل النهائي الذي يستهدفه الاعتداء, لكنه ليس تقسيما منضبطا و لا هو تقسيم محددا, فالجرائم التي تستهدف الأموال تضم من حيث مفهومها السرقة و الاحتيال , أما الجرائم التي تستهدف التزوير فتمس الثقة و الاعتبار, والجرائم الواقعة ضد الآداب قد تتصل بالشخص و قد تتصل بالنظام و الأخلاق العامة, و على العموم فانه وتبعا لهذا التقسيم الوارد ضمن مشروع القانون النموذجي الأمريكي , تصنف جرائم الكمبيوتر على النحو التالي:

1- قانون وضع عام 1998م من قبل بحث أكاديمي بالولايات المتحدة الأمريكية و المسمى:
Model static computer crimes code

أولا : " طائفة الجرائم التي تستهدف الأشخاص "

و تشمل القتل بالكمبيوتر(Computer murder), و التسبب بالوفاة, جرائم الإهمال المرتبطة بالكمبيوتر والتحريض على الانتحار, و التحريض القصدي للقتل عبر الانترنت, التحرش و المضايقة عبر وسائل الاتصال المؤتمنة، التهديد عبر وسائل الاتصال المؤتمنة، الإحداث المتعمد للضرر العاطفي أو التسبب بضرر عاطفي عبر وسائل التقنية , الملاحقة عبر وسائل التقنية , أنشطة اختلاس النظر أو الإطلاع على البيانات الشخصية , قنابل البريد الالكتروني, أنشطة صنع البريد الالكتروني غير المطلوب أو غير المرغوب به , بث المعلومات المضللة أو الزائفة و الانتهاك الشخصي لحرمة الكمبيوتر(غير المصرح به).

ثانيا:" طائفة جرائم الأموال- عدا السرقة- أو الملكية المتضمنة أنشطة الاختراق و الإتلاف"

Property and Crimes Involving Intrusions Damage (other than theft)

و تشمل أنشطة الاقتحام أو الدخول أو التوصل غير المصرح به مع نظام الكمبيوتر أو الشبكة إما مجردا أولجهة ارتكاب فعل آخر ضد البيانات و البرامج و المخرجات و تخريب المعطيات و النظم و الممتلكات ضمن مفهوم تخريب الكمبيوتر و إيذاء الكمبيوتر و اغتصاب الملكية و خلق البرمجيات الخبيثة و الضارة ونقلها عبر النظم و الشبكات و استخدام اسم النطاق أو العلامة التجارية أو اسم الغير دون ترخيص, وإدخال معطيات خاطئة أو مزورة إلى نظام كمبيوتر و التعديل غير المصرح به لأجهزة و معدات الكمبيوتر والإتلاف غير المصرح به لنظم الكمبيوتر, و أنشطة إنكار الخدمة أو تعطيل أو اعتراض عمل النظام أوالخدمات, و أنشطة الاعتداء على الخصوصية (و هذه تخرج عن مفهوم الجرائم التي تستهدف الأموال لكنها تتصل بجرائم الاختراق) , وإفشاء كلمة سر الغير, و الحيازة غير المشروعة للمعلومات , وإساءة استخدام المعلومات, و نقل معلومات خاطئة.

ثالثا : " جرائم الاحتيال و السرقة "

و تشمل جرائم الاحتيال, التلاعب بالمعطيات و النظم, و استخدام الكمبيوتر للحصول على أو استخدام البطاقات المالية للغير دون ترخيص أو تدميرها, و الاختلاس عبر الكمبيوتر أو بواسطته, و سرقة معلومات الكمبيوتر و قرصنة البرامج, و سرقة خدمات الكمبيوتر (وقت الكمبيوتر), و سرقة أدوات التعريف والهوية عبر انتحال هذه الصفات أو المعلومات داخل الكمبيوتر.

رابعا : « جرائم التزوير"

و تشمل تزوير البريد الالكتروني (E – Mail forgery) و تزوير الوثائق و السجلات /Document) (Record forgery و تزوير الهوية (Identity forgery).

خامسا : " جرائم المقامرة و الجرائم الأخرى ضد الآداب و الأخلاق"

و تشمل تلك إدارة مشروع مقامرة على الانترنت, و تسهيل إدارة مشاريع القمار على الانترنت و تشجيع مشروع مقامرة عبر الانترنت و استخدام الانترنت لترويج الكحول و مواد الإدمان للقصر.

سادسا : " جرائم الكمبيوتر ضد الحكومة "

و تشمل هذه الطائفة كافة جرائم تعطيل الأعمال الحكومية و تنفيذ القانون, و الإخفاق في الإبلاغ عن جرائم الكمبيوتر و الحصول على معلومات سرية, و الإخبار الخاطىء عن جرائم الكمبيوتر, و العبث بالأدلة القضائية أو التأثير فيها و تهديد السلامة العامة و بث البيانات من مصادر مجهولة, كما تشمل الإرهاب الالكتروني أو أنشطة تطبق القانون بالذات.

الفرع الرابع : " تصنيف الجرائم كجرائم الكمبيوتر و جرائم الانترنت "

تبعا للتطور التكنولوجي و التحول التاريخي من حيث أجهزة الكمبيوتر و المعلوماتية بصفة عامة, من الطبيعي أن يكون ثمة مفهوم لجرائم ترتكب على الكمبيوتر قبل أن يشيع استخدام شبكات المعلومات, وتحديدا الانترنت, فهذه الأخيرة تخلق أنماط جرمية مستجدة.

طال معالجة و التخزين و الاسترجاع, و بين الأنشطة التي تستهدف الشبكات ذاتها أو معلومات المنقولة عبرها, فمن خلال كل هذا نجد البعض يحصر أنشطة جرائم الانترنت بتلك المتعلقة بالاعتداء على الموقع وتعطيلها أو تشويهها أو تعطيل تقديم الخدمة, و أنشطة الاستيلاء على كلمات سر المستخدمين, و أنشطة نشر الفيروسات المعلوماتية و أنشطة الاعتداء على محتوى المواقع و التصميم و غيرها من الجرائم التي يجمعها مفهوم (جرائم الملكية الفكرية عبر الانترنت).

و يجري التمييز بين الأفعال التي تستهدف المعلومات في نطاق نظام الكمبيوتر خلال مراحل المعالجة والتخزين و الاسترجاع، و بين الأنشطة التي تستهدف الشبكات ذاتها أو المعلومات المنقولة عبرها، فمن خلال كل هدا نجد البعض يحصر أنشطة جرائم الانترنت بتلك المتعلقة بالاعتداء على المواقع و تعطيلها أوتشويهها أو تعطيل تقديم الخدمة، و أنشطة الاستيلاء على كلمات سر المستخدمين، و أنشطة نشر الفيروسات المعلوماتية و أنشطة الاعتداء على محتوى المواقع و التصميم و غيرها من الجرائم التي يجمعها مفهوم (جرائم الملكية الفكرية عبر الانترنت).

أما جرائم الكمبيوتر فإنها تعاد إلى الأنشطة التي تستهدف المعلومات و البرامج المخزنة داخل نظم الكمبيوتر و تحديدا أنشطة التزوير و احتيال الكمبيوتر و سرقة وقت الحاسوب, إضافة للتدخل غير

المصرح به و الذي يتوزع بين الدخول غير المصرح به لنظام الكمبيوتر و الدخول غير المصـــرح بـــه للشبكات, فيتبع لمفهوم الجرائم المعلوماتية عبر الانترنت, لأنه في كلا الحالتين هو دخـــول إلـــى نظـــام الكمبيوتر عبر الشبكة, فلو أخذنا مثال: جريمة تعطيل عمل نظام كمبيوتر أم موقع انترنت فهي تســـتهدف نظام الكمبيوتر الذي هو في الحالة الأولى كمبيوتر مغلق و في الثانية كمبيوتر يدير موقع انترنت.

الفصل الثاني

ميكانزمات و دوافع ارتكاب الجريمة المعلوماتية

الفصل الثاني : "ميكانيزمات و دوافع ارتكاب الجريمة المعلوماتية"

ليس ثمة أصدقاء في العالم الالكتروني، وصغيرا لمجرمين ككبير هم، و المازح من بينهم كالحاقد، وضمان أمن المعلومات وضمان عدم التعرض يوجب التعامل مع الكلّ على أنّهم مصدر للخطر، وليست المسألة إهدار لفكرة حسن النية أو الثقة بالآخرين، إنّما الضمان الوحيد للحماية من مصادر خطر بالغة قد تؤدي إلى خسائر لا يمكن تقديرها أو تجاوزها.

ما من شك أن المدى الزمني لنشأة وتطور العلوم الجنائية، حمل معه نشوء وتطور و اندثار نظريات عدّة في مجال علم الإجرام و في مجال تصنيف المجرمين، و أنساب الجنوح والانحراف، و أمكن في ظل هذه العلوم، وما نتج في نطاقها من دراسات في ميدان علم الإجرام تحديدا، بلورة سمات عامة للمجرم عموما، وسمات خاصة يمكن استظهارها لطائفة معينة من المجرمين، تبعا للجرائم التي يرتكبونها، فكان من الطبيعي أن تحمل ظاهرة الجرائم المعلوماتية في جنباتها ولادة طائفة من المجرمين، مجرمو المعلوماتية، تتوافر فيهم سمات عامة بغض النظر عن الفعل المرتكب وسمات خاصة تبعا للطبيعة المميزة لبعض جرائم المعلوماتية والأغراض المراد تحقيقها.

و الحقيقة أنه وحتى الآن، لم تتضح الصورة جليّة في شأن تحديد صفات مرتكبي الجرائم المعلوماتية و استظهار سماتهم، وضبط دوافعهم، نظرا لقلة الدراسات الخاصة بالظاهرة برمتها من جهة، ونظرا لصعوبة الإلمام بمداها الحقيقي، بفعل الحجم الكبير من جرائمها غير المكتشف، أو التي لم تتم بشأنها ملاحقة قضائية رغم اكتشافها لصعوبة إثباتها أو للنقص التشريعي الذي يحدّ من توفير الحماية الجنائية في مواجهتها.

المبحث الأول: " مرتكبي الجرائم المعلوماتية"

في بداية الظاهرة شاع الحديث عن المجرمين الصغار الدين يرتكبـون مختلـف أنـواع الاعتداءات على نظم الكمبيوتر و تحديدا الاختراقات بدافع التحدي و إثبات المقدرة العلمية و التقنية، و كان ثمة حديث عن استغلال ميول التحدي لديهم و أحيانـا احتياجـاتهم الماديـة لتسخيرهم للقيام بأنشطة جرمية تتصل بالتقنية تدر منافع لمنظمات الجريمـة، و مـع تنـامي الظاهرة و تعدد أنماط هده الجرائم، و نشوء أنماط جديدة متصلة بشبكات الكمبيوتر و تحديـدا الانترنت، اتجهت جهات البحث و تحديدا الهيئات العاملة في ميدان السلوك الإجرامي لمحاولة تصنيف مرتكبي جرائم المعلوماتية و الانترنت و بيان السمات الأساسية لكل فئة بغرض بحث أنجع الوسائل لردع هده الفئات أو الحد من نشاطها، باعتبار دلك من المسـائل الموضـوعية اللازمة لتحديد اتجاهات المكافحة.

المطلب الأول : " صفات مرتكبي الجريمة المعلوماتية"

إن دراسات علم الإجرام الحديثة في ميدان إجرام التقنية تسعى في الوقت الحاضر إلى إيجـاد تصنيف منضبط لمجرمي المعلوماتية لكنها تجد صعوبة في تحقيق دلك بسبب التغير السـريع الحاصل في نطاق هده الظاهرة و المرتبط أساسا بالتسارع الرهيب في ميدان الكمبيوتر و الانترنت، فالمزيد من الوسائل و المخترعات و الأدوات التقنية يساهم فـي تغيـر أنمـاط الجريمة و تطور و فعالية وسائل الاعتداء، و هدا بدوره يساهم في إحـداث تغيـرات علـى السمات التي يتصف بها مجرمي المعلوماتية، على الأقل السمات المتصلة بالفعل نفسه و لـيس بالشخص، و لهدا يتجه الباحثون مؤخرا إلى الإقرار بأن أفضل تصنيف لمجرمي المعلوماتيـة هو التصنيف القائم على أساس أغراض الاعتداء و ليس على أساس التقنية أو علـى أسـاس الوسائط محل الاعتداء أو المستخدمة لتنفيذه.

ويعدّ من أفضل التصنيفات لمجرمي المعلوماتية، التصنيف الـذي أورده Vontorch David Icove, Karl seger et william "1".

حيث تم تقسيم مجرمي التقنية إلى ثلاث طوائف: المخترقون والمحترفون و الحاقدون، كما أن من بين التصنيفات الهامة التمييز بين صغار السن من مجرمي المعلوماتية وبين البالغين الذين يتجهون للعمل معا لتكوين المنظمات الإجرامية الخطرة.

الفرع الأوّل: " المخترقون والمتطفلون"

إن لاصطلاح الهاكرز (المخترقون) والكراكرز (المتطفلون) تباينا جوهريا، فالهاركز متطفلون يتحدّون إجراءات أمن النظم و الشبكات، لكن لا تتوافر لديهم في الغالـب دوافـع حاقـدة أو تخريبية وإنّما ينطلقون من دوافع التحدّي وإثبات المقدرة، أما الكريكرز فإن اعتداءاتهم تعكـس ميولا جريمة خطرة تنبئ عنها رغباتهم في إحداث التخريب، و مع أن المعيار غير منضبط إلا أن الدراسات والمعالجات في حقل جرائم المعلوماتية، بل بعـض التشـريعات المحليـة فـي الولايات المتحدّة الأمريكية تعتمد هذا التمييز، فاصطلاح الكريكرز مرادف للهجمات الحاقدة و المؤدية في حين أن اصطلاح الهاكرز مرادف في الغالب لهجمات التحـدّي طبعـا دون أن يؤثر هذا التمييز على مسؤولية مرتكبي الأنشطة من كلا الطائفتين ومساءلتهم عما يلحقونه من أضرار بالمواقع المستهدفة باعتداءاتهم، هذا إضافة إلى أن الاصطلاحين يختلفون واقعيا ومـن حيث الأساس التاريخي لنشأة كلّ منهما، وأفراد هذه الطائفة يرتكبون الجرائم بـدافع التحـدي الإبداعي ويجدون أنفسهم متفقين إلى درجة أنّهم ينصّبون أنفسهم أوصـياء علـى أمـن نظـم الكمبيوتر في المؤسسات المختلفة، والسّمة الغالبة على أعضاء هذه الطائفة صغار السن، قلـة الخبرة وعدم التمييز بين الأنظمة محل الاختراق – طبعا يتميّز الكريكرز عن الهـاكرز فـي مستوى المعرفة التقنية –

1- تصنيف وارد في مؤلفهم " جرائم الكمبيوتر"، الصادر عام 1995.

وبرغم هذه السمات فقد تمكن المجرمون من هذه الطائفة من اختراق مختلف أنواع نظم الكمبيوتر التابعة للشركات المالية و التقنية و البنوك ومصانع الألعاب والمؤسسات الحكومية ومؤسسات الخدمة العامة وكثر الحديث عن وقائع عملية كما في حالة اختراق أحد الصبية الذي يبلغ من العمر 14 عاما، نظام الكمبيوتر العائد للبنتاغون و الآخر لا يتجاوز عمره السابعة عشرة تمكن من اختراق كمبيوترات العديد من المؤسسات الاستراتيجية في أوروبا والولايات المتحدّة الأمريكية.

والسمة المميزة الأخرى لهذه الطائفة تبادلهم للمعلومات فيما بينهم وتحديدا التشارك في وسائل الاختراق وآليات نجاحها وإطّلاعهم بعضهم البعض على مواطن الضعف في نظم الكمبيوتر والشبكات، حيث تجري عمليات التبادل للمعلومات فيما بينهم وبشكل رئيسي عن طريق النشرات الإعلامية الإليكترونية ومجموعات الأخبار، وفي تطور حديث لتنظيم هذه الطائفة نفسها يجري عقد مؤتمرات لمخترعي الكمبيوتر يدعى له الخبراء من بينهم للتشاور حول وسائل الاختراق ووسائل تنظيم عملهم فيما بينهم و بالرغم من أنّ الخطورة في هؤلاء تكمن بمثابرتهم على أنشطة الاختراق وتطوير معارفهم التقنية، وبالرغم من توفر فرصة استغلال هؤلاء من قبل منظمات وهيئات إجرامية تسعى للكسب المادّي فإنّه ومن ناحية أخرى ساهم العديد من هؤلاء المخترقين في تطوير نظم الأمن في عشرات المؤسسات في القطاعين الخاص والعام، حتى أن العديد من الجهات تستعين بخبراتهم في أحيان كثيرة في فحص وتدقيق مستوى أمن نظم الكمبيوتر والمعلومات.

هل الهاركز مجرمون؟؟

ثمة خلط كبير، تحديدا في المواد التي تتناقلها الصحف و المجلات و الوسائل الإعلامية بين مجرمي التقنية وبين الهاركز، وقد وصل الخلط إلى حد اعتبار كلّ من ارتكب فعلا من أفعال الاعتداء المتصلة بجرائم المعلوماتية و الانترنيت من قبيل الهاكرز، ربما لأن غالبية الاعتداءات تتم عن طريق الدخول غير المصرح به عبر شبكات المعلومات وتحديدا الانترنت، لكن الحقيقة غير ذلك.

حتى أن هناك من يدافع عن مجموعات الهاكرز التي لا تمارس أيّة افعـال تسـتهدف الحـاق الضرر بالغير انطلاقا إلى ان اغراض الاختراق لديهم تنحصر في الكشف عن الثغرات الأمنية في النظام محلّ الإعتداء، وثمّة من يؤكد من بين الهـاركز المحتـرفين أن لـديهم ضـوابط وأخلاقيات خاصة بهم، بل أن العديد من مواقع الأنترنيت التي تهتم بمسائل الهـاكرز أنشـأها بعضهم ويعرضون فيها لمواد تتصل بتوضيح حقيقة هؤلاء ومحاولة سلخ أيّـة صـفة غيـر مشروعة أو جرمية عن الأنشطة التي يقومون بها.

ومع ذلك فإن علينا أن نقر بخطورة الهاكرز الذين تربوا في اجواء تحديات الاختراق والتفاخر بإبداعاتهم في هذا الحقل و الذين يتم استغلالهم من قبل مجموعات الجريمة المنظمة لإرتكـاب أفعال مخطط لها، فعنصر التحدي القائم لديهم لايترك لديهم وازعا للتراجع ولايتيح لهم التمييز أو تقليب الأمور، وليس لديهم ضوابط بشأن النشاط الذي يقومون به النظام الذي يخترقونه.

الفرع الثاني : "مجرمو المعلوماتية المحترفون"

تتميز هذه الطائفة بسعة الخبرة والإدراك الواسع للمهارات التقنيـة، كمـا تتميّـز بـالتنظيم والتخطيط للأنشطة التي ترتكب من قبل أفرادها، ولذلك فإن هذه الطائفة تعد الأخطر من بـين مجرمي التقنية حيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم أو للجهات التي كلفتهم و سخرتهم لارتكاب جرائم المعلوماتية كما تهدف اعتداءات بعضهم إلى تحقيق أغراض سياسية و التعبير عن موقف فكري أو نظري أو فلسفي.

ويتم تصنيف أفراد هذه الطائفة إلى مجموعات متعددة، إمّا تبعا لتخصصهم بنوع معـين مـن الجرائم أو تبعا للوسيلة المتبعة من قبلهم في ارتكاب الجرائم، فمـثلا نجـد طائفـة محترفـي التجسّس الصناعي وهم أولئك الذين يوجهون أنشطتهم إلى اختراق نظم المعلوماتيـة العائـدة للشركات الصناعية ومشاريع الأعمال بقصد الاستيلاء على الأسرار الصناعية والتجارية إمـا

لحساب أعمال يقومون بها بذاتهم أو في الغالب لحساب منافسين آخرين في السوق وأحيانا لحساب مجموعات القرصنة الدولية.

ونجد مثلا طائفة مجرمي الاحتيال و التزوير، وهؤلاء هم الطائفة التي تكون أغراضها متجهة إلى تحقيق كسب مادي والاستيلاء على أموال الآخرين، وضمن هذه الطائفة أيضا ثمّة تصنيفات عديدة، فمنهم محتالو شبكات الهاتف، محتالو الانترنيت وغير ذلك، وحتى في الطائفة الفرعية، قد تتوفر تخصصات لبعضهم كأن يوجه الشخص أنشطته الاحتيالية إلى قطاع مزادات البضاعة والمنتجات على الانترنيت أو في ميدان الاستيلاء على أرقام بطاقات الائتمان و الاتجار بها.

و إلى جانب المعرفة التقنية المميّزة و التنظيم العالي و التخطيط للأنشطة المنوي ارتكابها، فإن أفراد هذه الطائفة يتسمون بالتكتم خلافا للطائفة الأولى فلا يتبادلون المعلومات بشأن أنشطتهم بل يطورون معارفهم الخاصة ويحاولون ما أمكن عدم كشف طرقهم التقنية لارتكاب جرائمهم، وحول الأعمار الغالبة على هذه الطائفة فإن الدراسات تشير إلى أنّهم من الشباب الأكبر سنّا من الطائفة الأولى وأن معظمهم تتراوح أعمارهم ما بين 25 و 40 عام.

الفرع الثالث : " الحاقدون"

هذه الطائفة يغلب عليها عدم توفر أهداف و أغراض الجريمة المتوفرة لدى الطائفتين المتقدمتين، فهم لا يسعون إلى إثبات المقدرات التقنية و المهارة وبنفس الوقت لا يسعون إلى مكاسب مادية أو سياسية، إنما يحرك أنشطتهم الرغبة بالانتقام و الثأر كأثر لتصرف صاحب العمل معهم أو لتصرف المنشأة المعينة معهم عندما لا يكونوا موظفين فيها، ولهذا فإنهم ينقسمون إما إلى مستخدمي للنظام بوصفهم موظفين أو مشتركين أو على علاقة ما بالنظام محل الجريمة، وإلى غرباء عن النظام تتوفر لديهم أسباب الانتقام من المنشأة المستهدفة في نشاطهم.

ولا يتسم أعضاء هذه الطائفة بالمعرفة التقنية الاحترافية، ومع ذلك يشقى الواحد منهم في الوصول إلى كافة عناصر المعرفة المتعلقة بالفعل المخصوص الذي ينوي ارتكابه، وتغلب على أنشطتهم من الناحية التقنية استخدام تقنيات زراعة الفيروسات و البرامج الضارة وتخريب النظام أو إتلاف كل أو بعض معطياته، أو نشاط إنكار الخدمة وتعطيل النظام أو الموقع المستهدف إن كان من مواقع الانترنيت.

وليس هناك ضوابط محددة بشأن أعمارهم، كما أنه لا تتوفر عناصر التفاعل بين أعضاء هذه الطائفة، و لا يفاخرون بأنشطتهم بل يعمدون إلى إخفائها، وهم الطائفة الأسهل من حيث كشف الأنشطة التي قاموا بارتكابها لتوفر ظروف وعوامل تساعد في ذلك.

وبالرغم من أن سمات هذه الطائفة تصنعها من حيث الخطورة في مؤخرة الطوائف المتقدمة إذ هم أقل خطورة من غيرهم من مجرمي التقنية، لكن ذلك لا يمنع أن تكون الأضرار التي نجمت عن أنشطة بعضهم جسيمة ألحقت خسائر فادحة بالمؤسسات المستهدفة.

الفرع الرابع : "طائفة صغار السنّ"

فئة صغار السن، أو كما يسميهم البعض "صغار نوابغ المعلوماتية" ويصفهم بأنهم « الشباب البالغ المفتون بالمعلوماتية و الحاسبات الآلية » "**1**"

فإن من بينهم في الحقيقة، فئة لم تزل دون سن الأهلية مولعين بالحوسبة و الاتصال، وقد تعددت أوصافهم في الدراسات الاصطلاحية، وشاع في نطاق الدراسات الإعلامية و التقنية وصفهم بمصطلح «المتلعثمين»، الدال حسب تعبير الأستاذ توم فور ستر على «الصغار المتحمسين للحاسوب، بشعور من البهجة، دافعهم التحدي لكسر الرموز السرية لتركيبات الحاسوب» "**2**"

1- الدكتور سامي الشوا، الغش المعلوماتي كظاهرة إجرامية مستحدثة، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25 – 28 أكتوبر 1993، ص 7.

2- Tom forester, essential problems to hig- tech society, first mit pres edition, Cambridge, massachusetts, 1989, p 405.

ويسميهم البعض كذلك بالمجانين بالاستناد إلى كثرة استخدام لتقنية المعدل و المعدل العكسي (الموديم) "modem"**1**"، ويثير مجرمو المعلوماتية من هذه الطائفة جدلا واسعا، ففي الوقت الذي كثر الحديث فيه عن مخاطر هذه الفئة، على الأقل بمواصلتها العبث بالحواسيب، ظهرت دراسات ومؤلفات تدافع عن هذه الفئة، لتخرجها من دائرة الإجرام إلى دائرة العبث، وأحيانا البطولة.

من هذه المؤلفات على سبيل المثال: كتاب " خارج نطاق الدائرة الداخلية- كيف تعملها" لمؤلفه الأمريكي " لبيل لاندريت"، و كتاب " الدليل الجديد للمتلعثمين" لمؤلفه " هوجو كورت" في المملكة المتحدة، وكتاب "المتلعثمون – أبطال ثورة الحاسوب" لمؤلفه "ستيفن ليفي" "**2**".

ومن الأمثلة الشهيرة لجرائم المعلوماتية التي ارتكبت من هذه الفئة العصابة الشهيرة التي أطلق عليها (عصابة 414) و التي نسب إليها ارتكاب ستون فعل تعدي في الولايات المتحدة الأمريكية على ذاكرات الحواسب،نجم عنها أضرار كبيرة لحقت بالمنشآت العامة و الخاصة. وكذلك، تلاميذ المدرسة الثانوية في ولاية (منهاتن) الذين استخدمو في عام 1980 طرفيات غرف الدرس للدخول إلى شبكة اتصالات وبيانات كثير من المستخدمين ودمروا ملفات زبائن الشركة الرئيسية في هذه العملية. كما سبب متلعثموا ألمانيا الغربية الصغار في عام 1984 فوضى شاملة، عندما دخلوا إلى شبكة (الفيديوتكس) ونجح بعض المتلعثمون الفرنسيون في ايجاد مدخل إلى الملفات السرية لبرنامج ذري فرنسي"**3**".

1- جهاز يعتمد على الاتصال الهاتفي لاختراق شبكة النظم و الاتصال بشبكة الانترنيت.

2- توم فور ستر، المرجع السابق، ص 407.

3- توم فور ستر، المرجع السابق، ص 409.

و يمكن رد الاتجاهات التقديرية لطبيعة هده الفئة و سمات أفرادها و مدى خطورتهم في نطاق ظاهرة جرائم المعلوماتية إلى ثلاث اتجاهات:

الأول :

اتجاه لا يرى أية صفة جرمية على هده الفئة، أو على الأفعال التي تقوم بها، و لا يرى وجوب تصنيفهم ضمن الطوائف الإجرامية لمجرمي المعلوماتية، استنادا إلى أن صغار السن "المتلعثمين" "لديهم ببساطة ميل للمغامرة و التحدي و الرغبة في الاكتشاف، و نادرا ما تكون أهداف أفعالهم المحظورة غير شرعية، و استنادا إلى أنهم لا يدركون و لا يقدرون مطلقا النتائج المحتملة التي يمكن أن تؤدي إليها أفعالهم غير المشروعة بالنسبة لنشاط منشأة أو شركة" "**1**".

الثاني :

الاتجاه الذي يحتفي بهده الفئة و يناصرها و يعتبرها ممن يقدم خدمة لأمن المعلومات و وسائل الحماية و يصفهم بالأخيار و أحيانا بالأبطال الشعبيين و يتمادى هدا الاتجاه في تقديره لهده الفئة بالمطالبة بمكافئتهم باعتبارهم لا يسببون ضررا للنظام، ولا يقومون بأعمال احتيال،

وينسب إليهم الفضل في كشف الثغرات الأمنية في تقنية المعلومات، ومثل هذا الرأي قال به أحد أشهر المدافعين على المخترقين الصغار "هيوجوكورن" وعكس أفكاره في مؤلفه "الدليل الجديد للمتلعثمين" وبسبب خطورة ما يشيعه "هيوجوكورن" ثم منع مؤلفه المذكور من قبل مركز بوليس مدينة لندن الكبرى "سكوتلانديارد" غير أن هذا المنع كان له أثر في توسيع دائرة انتشار هذا الكتاب وتحقيق نسبة عالية جدا من المبيعات. "**2**"

ويتمادى الإعلامي "ستيفن ليف" في الاحتفال بهذه الفئة، واصفا إياهم بأبطال ثورة الحاسوب متحمسا لهذا الوصف إلى درجة إطلاقه عنوانا على مؤلفه الخاص بهذه الظاهرة، لا لموقف

1- د.الشوا، ورقة عمل، السابق، ص 08.

2- توم فورستر، المرجع السابق، ص 401 و 32.

معادٍ من التقنية، بل لأنه يرى في دوافعهم الخيرة لا الشريرة، الموجهة لمالكي الأموال لا المحتاجين، ما ينهض بوصفهم بالأبطال الشعبيين."**1**"

الثالث :

اتجاه يرى أن مرتكبي جرائم المعلوماتية من هذه الطائفة، يصنعون مجرمي المعلوماتية كغيرهم دون تمييز استنادا إلى أن تحديد الحدّ الفاصل بين العبث في الحواسيب وبين الجريمة أمر عسير من جهة، ودونما أثر على وصف الفعل –قانونا– من جهة أخرى، واستنادا إلى أن خطورة أفعالهم التي تتميز بانتهاك الأنظمة واختراق الحواسيب وتجاوز إجراءات الأمن، والتي تعد بحق من أكثر جرائم المعلوماتية تعقيدا من الوجهة التقنية، عوضا عن مخاطرها المدمرة.

ويدعم صحة هذا الاتجاه التخوفات التي يثيرها أصحاب الاتجاه الأول ذاتهم، إذ يخشون من الخطر الذي تواجهه هذه الطائفة، والمتمثل باحتمال الانزلاق من مجردها وصغير لاقتراف الأفعال غير المشروعة، إلى محترف لأعمال السلب، هذا إلى جانب خطر آخر أعظم، يتمثل في احتضان منظمات الإجرام ومجرمين غارقين في الإجرام لهؤلاء الشباب.

الفرع الخامس : "المجرمون البالغون – محترفو الإجرام"

إن مرتكبي جرائم المعلوماتية عموما، ينتمون وفق الدراسات إلى فئة عمرية تتراوح ما بين (25 – 45) عاما، وبالتالي، يمتاز مرتكبو هذه الجرائم بصفات الشباب العمرية والاجتماعية، وإذا استثنينا صغار السن من بينهم، الذين تكون أعمارهم دون الحد الأدنى المشار إليه أعلاه، عمّا رأينا فيما سلف، فإن لمجرمي المعلوماتية سمات عامة، يتحقّق بعضها لدرجة أقل في صغار السن وهذه السمات إضافة لما أوردناه في الطوائف المتقدمة، تتمثل بما يلي:

1– توم فورستر، المرجع السابق، ص 405.

أولا : "الصفات الشخصية والتخصص والكفاءة"

الجامع بين محترفي جرائم المعلوماتية وتمتعهم بقدرة عالية من الذكاء، وإلمام جيد بالتقنية العالية، واكتسابهم معارف عملية وعالمية، وانتمائهم إلى التخصصات المتصلة بالحاسوب من الناحية الوظيفية، وهذه السمات تتشابه مع سمات مجرمي ذوي "الياقات البيضاء" "**1**".

أما فيما يتعلق بكفاءة مجرمي المعلوماتية، فإن الدراسات القليلة المتوفرة تشير إلى تمتعهم بكفاءة عالية، إلى درجة اعتبارهم مستخدمين مثاليين من قبل الجهات العاملين لديها، وممن يوسمون بالنشاط الواسع والإنتاجية الفاعلة.

ثانيا : "من حيث الجوانب السيكولوجية"

إن الدراسات القليلة للجوانب السيكولوجية لمجرمي المعلوماتية، أظهرت شيوع عدم الشعور بلا مشروعية الطبيعة الإجرامية وبلا مشروعية الأفعال التي يقترفونها، كذلك الشعور بعدم استحقاقهم للعقاب عن هذه الأفعال، فحدود الشرّ والخير متداخلة لدى هذه الفئة، وتغيب في داخلهم مشاعر الإحساس بالذنب، وهذه المشاعر في الحقيقة تبدو متعارضة مع ما تظهره الدراسات من خشية مرتكبي جرائم المعلوماتية من اكتشافهم و افتضاح أمرهم ولكن هذه الرهبة والخشية يعكسها انتمائهم في الأعم الأغلب إلى فئة اجتماعية متعلمة ومثقفة."**2**"

1- يقول د.جميل عبد الباقي أن "مرتكبي الجرائم المعلوماتية يتميزون في غالب الأحيان بأنهم أفراد ذات مكانة في المجتمع، و يتمتعون بقدر كاف من العلم، و دلك أمر طبيعي من حيث أن تنفيذ هده الجرائم يستلزم إلماما كافيا بمهارات و معارف فنية في مجال أنظمة الحاسب الآلي وكيفية تشغيله، الأمر الذي يدعونا إلى القول بأن مرتكبي هده الجرائم دائما ما يكونوا من المتخصصين في مجال معالجة المعلومات أليا"، المرجع السابق، ص 15.

2- يقول د.سامي الشوا: "إن الاستخدام المتزايد للحاسبات الآلية، قد أنشأ مناخا نفسيا مواتيا لتصور استبعاد فكرة الخير و الشر، و ساعد على دلك عدم وجود احتكاك مباشر بالأشخاص و سيادة التباعد و التمزق في العلاقة الثنائية بين الفاعل و المجني عليه الذي بدوره أدى إلى تهدئة الوسوسة المحتملة، و سهل فيما يبدو المرور إلى الفعل غير المشروع و خلق لديهم نوعا من الإقرار الشرعي الذاتي، مع هدا يجب أن لا نسبح في الخيال، حيث لا يمكن أن ننكر أن من بين الحالات التي خضعت للبحث وجد عدد كبير من مرتكبي جرائم الغش المعلوماتي لديه اتجاه إجرامي خطير، و دي نية سيئة جلية، و يبرز دلك على وجه الخصوص في بعض الأعمال التي لها طابع المنافسة الشرسة و التي تشمل المجرمين المحنكين و أيضا في نطاق أعمال التجسس"، السابق، ورقة عمل، ص 09.

المطلب الثاني : "دوافع ارتكاب الجريمة المعلوماتية"

الدافع (الباعث)، الغرض، الغاية، تعبيرات لكل منها دلالته الاصطلاحية في القانون الجنائي، تتصل بما يعرف بالقصد الخاص في الجريمة، وهي مسألة تثير جدلا فقهيا وقضائيا واسعا، ذلك أن "القاعدة القضائية تقرر أن الباعث ليس من عناصر القصد الجرمي" "**1**". وإن الباعث "لا أثر له في وجود القصد الجنائي" "**2**". وإذا كان الاستخدام العادي للتعبيرات المشار إليها يجري على أساس ترادفها في الغالب، فإنها من حيث الدلالة تتمايز وينتج عن تمايزها آثار قانونية على درجة كبيرة من الأهمية، فالباعث (الدافع) هو "العامل المحرك للإدارة الذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والانتقام" "**3**". وهو إذن قوة نفسية تدفع الإدارة إلى الاتجاه نحو ارتكاب الجريمة ابتغاء تحقيق غاية معينة وهو "يختلف من جريمة إلى أخرى، تبعا لاختلاف الناس من حيث السّن والجنس ودرجة التعليم وغير ذلك من المؤثرات كما يختلف بالنسبة للجريمة الواحدة من شخص لآخر" "**4**".

أما الغرض "فهو الهدف الفوري المباشر للسلوك الإجرامي ويتمثل بتحقيق النتيجة التي انصرف إليها القصد الجنائي أو الاعتداء على الحق الذي يحميه قانون العقوبات" "**5**". وأما الغاية " فهي الهدف البعيد الذي يرمي إليه الجاني بارتكاب الجريمة كإشباع شهوة الانتقام أو سلب مال المجني عليه في جريمة القتل" "**6**".

1- د.نجيب حسني، القسم العام، السابق، ص 1052.

2- الأستاد الدكتور أحمد فتحي سرور، الوسيط في قانون العقوبات، القسم العام، الطبعة الخامسة، دار النهضة العربية، القاهرة، 1991، ص 427.

3- د.كامل السعيد، القسم العام، السابق، ص 226.

4- الدكتورة فوزية عبد الستار، شرح قانون العقوبات- القسم العام، الطبعة الخامسة، دار النهضة العربية، القاهرة، 1991، ص 479.

5- د.السعيد، السابق، ص 226.

6- د.السعيد، السابق، و د.حسني، اسابق.

و الأصل أن الباعث والغاية ليس لهما أثر قانوني قي وجود القصد الجنائي الذي يقوم على عنصرين، علم الجاني بعناصر الجريمة، واتجاه إرادته إلى تحقيق هذه العناصر أو إلى قبولها، ولا تأثير للباعث أو الغاية "على قيام الجريمة أو العقاب عليها، فالجريمة تقوم بتحقيق عناصرها سواء كان الباعث نبيلا أو رذيلا و سواء كانت الغاية شريفة أو دنيئة، و إدا كانت القاعدة أن الباعث أو الغاية لا أثر لهما على قيام الجريمة، فإن القانون يسبغ عليهما في بعض الأحيان أهمية قانونية خاصة" "**1**".

و بالنسبة لجرائم الكمبيوتر و الانترنيت، فثمة دوافع عديدة تحرك الجناة لارتكاب أفعال الاعتداء المختلفة المنطوية تحت هذا المفهوم، ويمكننا من خلال الحالات التطبيقية تبين الدوافع الرئيسية التالية: "**2**".

<u>الفرع الأول</u> : "السعي إلى تحقيق الكسب المالي"

يعد هذا الدافع (والذي يمثل في الحقيقة غاية الفاعل) من بين أكثر الدوافع تحريكا للجناة لاقتراف جرائم المعلوماتية، ذلك أن خصائص هذه الجرائم، وحجم الربح الكبير الممكن تحقيقه من بعضها، خاصة غش الحاسوب أو الاحتيال المرتبط بالحاسوب، يتيح تعزيز هذا الدافع.

ومنذ بدايات الظاهرة، فإن الدراسات أشارت إلى أن المحرك الرئيسي لأنشطة احتيال الكمبيوتر، وفيما بعد احتيال الانترنيت، هو تحقيق الكسب المالي، ففي دراسة قديمة عرض لها الفقيه parker، يظهر أن 43% من حالات الغش المرتبط بالحاسوب المعلن عنها قد بوشرت من أجل اختلاس المال، وهي النسبة الأعلى من بين النسب التي حققتها جرائم أخرى في هذه الدراسة (32 % سرقة معلومات، 19 % أفعال إتلاف، 15 % سرقة وقت الحاسوب (الآلة) لأغراض شخصية)."**3**"

1- د.حسني، السابق، ص 480.

2- يحدد الدكتور سامي الشوا دوافع رئيسية أربعة يعبر عنها بالأسباب الرئيسية لظاهرة الغش المعلوماتي، تتمثل بالشغف بالإلكترونيات و السعي إلى الربح و الدوافع الشخصية أو المؤثرات الخارجية و الأسباب الخاصة بالمنشأة، المرجع السابق.

3- يقول د. سامي الشوا: "في الواقع فإن المحرك لاقتراف فعل الغش المعلوماتي يمكن أن ينطلق من مجرد النجاة من غرق الديون المستحقة أو من المشاكل العائلية الراجعة إلى النقد، أو من الخسائر الضخمة لألعاب القمار أو من إدمان المخدرات، و قد تكون جميع الوسائل مشروعة في هده المرحلة و بالنسبة للبعض فالغاية تبرر الوسيلة".

وإذا ما انتقلنا للدراسات الحديثة، فسنجد أن الدافع يسود على غيره ويعكس استمرار اتجاه مجرمي التقنية إلى السعي لتحقيق مكاسب مادية شخصية، وفي مقدمة هذه الدراسات والتقارير الإحصائية، الدراسات والتقارير الصادرة عن مركز احتيال المعلومات الوطني في الولايات المتحدة الأمريكية NFIC

<u>الفرع الثاني</u> : "الانتقام من رب العمل و إلحاق الضرر به"

قد لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى، يتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل و المشكلات المالية، ومن طبيعة علاقات العمل المنفرة في حالات معينة، هذه الأمور قد تدفع إلى النزعة نحو تحقيق الربح، لكنها في حالات كثيرة، مثلث قوة محركة لبعض العاملين لارتكاب جرائم المعلوماتية، باعثها الانتقام من المنشأة أو رب العمل، وسنجد في معرض تناولنا لجرائم المعلوماتية، وتحديدا جرائم إتلاف البيانات، والبرامج، أمثلة كثيرة كان دافع الجناة فيها إشباع الرغبة بالانتقام، وتحتل أنشطة زرع الفيروسات المعلوماتية في نظم الكمبيوتر النشاط الرئيسي والتكنيك الغالب للفئة التي تمثل الأحقاد على رب العمل الدافع المحرك لارتكاب الجريمة.

<u>الفرع الثالث</u> : « الرغبة في قهر النظام والتفوق على تعقيد وسائل التقنية »

يرى البعض "**1**" « أن الدافع إلى ارتكاب الجرائم في الطائفة الأولى (جرائم المعلوماتية) يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح » ومع أن الدراسات لا تظهر هذه الحقيقة على إطلاقها، إذ يظهر السعي إلى تحقيق الربح دافعا أكثر تحريكا لجرائم المعلوماتية من الرغبة في قهر النظام إلا أن الدافع الأخير، يتجسد في نسبة معتبرة من جرائم المعلوماتية خاصة ما يعرف بأنشطة الهاكرز (Hackers) المتطفلين الدخيلين "**2**". على النظام و المتجسدة في جرائم التوصل مع أنظمة الحاسب تحديدا عن بعد، والاستخدام غير المصرح به لنظام الحاسوب، واختراق مواقع الانترنيت.

1- د.جميل عبد الباقي، السابق، ص 16.

2- حسب ترجمة غرفة التجارة العربية البريطانية، و الأستاذ كامل السعيد.

ويميل مرتكبو هذه الجرائم إلى إظهار تفوقهم ومستوى ارتقاء براعتهم لدرجة انه إزاء ظهـور أية تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم (شغف الآلة) يحاولوا إيجـاد، وغالبـا مـا يجدون الوسيلة إلى تحطيمها (والأصوب التفوق عليها).

ويتزايد شيوع هذا الدافع لدى فئة صغار السن من مرتكبي جرائم المعلوماتية، الذين يمضـون وقتا طويلا أمام حواسيبهم الشخصية في محاولة لكسر حـواجز الأمـن لأنظمـة الحواسـيب وشبكات المعلومات، ولإظهار تفوقهم على وسائل التقنية.

ونكتفي بالقول هنا أن هذا الدافع هو أكثر الدوافع التي يجري استغلالها من قبـل المنظمـات الجريمية (مجموعات الجريمة المنظمة الجهة استدراج محترفي الاختراق إلى قبول المشـاركة في أنشطة اعتداء معقدّة أو استئجارهم للقيام بالجريمة.

الفرع الرابع : "دوافع أخرى ودوافع متعددة"

هذه أبرز دوافع ارتكاب الجريمة المعلوماتية، لكنها ليست كل الدوافع فمحرك أنشطة الإرهاب الإلكتروني و حروب المعلومات، الدوافع السياسية و الإيديولوجيـة، فـي حـين أن أنشـطة الاستيلاء على الأسرار التجارية تحركها دوافع المنافسة، والفعل الواحد قد يعكس دوافع متعددة خاصة ما إذا اشترك فيه أكثر من شخص، انطلق كل منهم من دوافع خاصة تختلف عن غيره، ويمكننا أخيرا أن نضع التصور الرياضي التالي لدوافع بعض الهجمات الشائعة في حقل جرائم المعلوماتية والإنترنت."**1**"

- حروب المعلومات والإرهاب الإلكتروني = دوافع سياسية أو فكرية.
- إنكار الخدمة للمواقع التجارية والخدمية = التحدي وقهر النظام+أفعـال ثأريـة وأحقـاد موظفين+التنافسية بأنشطة غير مشروعة.

1- www.oecd.org

- احتيال الكمبيوتر واحتيال الإنترنت = استيلاء على المال أو المنافع وتحقيق الربح.
- الاستيلاء على المعلومات = التنافسية+ابتزاز الأفراد وتحقيق المكاسب+المنافع المالية+الأفعال الثأرية+الإعداد للهجمات ذات الدوافع المالية.
- إتلاف المعطيات وتخريب الأنظمة = الأحقاد والدوافع الثأرية+إخفاء الأنشطة الجريمة الأخرى+التنافسية غير المشروعة+التحدي وتحديدا بالنسبة لبرامج الفيروسات.

المبحث الثاني : "السمات المميزة لجرائم المعلوماتية ووسائل الحماية"

ربما سمعت في الأخبار عدّة مرات عن تصفية شخص من قبل هواة عبر الانترنيت وخسارة شخص لرصيده المالي بسرقة رقم بطاقته الائتمانية عبر الانترنيت، ووقع شخص آخر في مأزق كبير بسبب المواقع الإباحية التي استخدمت بطاقته الائتمانية لدخولها من خلال الانترنيت، وما هو أخطر من ذلك، ما تناقلته وسائل الإعلام قبل أيام من انتحار شخصين تعارفا عبر الانترنيت واتفقا على إطلاق النار كل منهما على الآخر لإحباطهما في الحياة، بل والأكثر خطورة جرائم الاختطاف والابتزاز و القتل، وسرقة الأموال، وتدمير المعلومات السريّة التي تضر باقتصاد الدول.

عند وجودك ضمن الانترنيت، تبرز مظاهر تسبب العديد من المشاكل، الشيء الذي يمكّنك عمل أو قول أي شيء ترغب به اتجاه الأشخاص الذين لا يعرفونك ولا يروك، وهو كون الانترنيت غير حقيقية، فبالنسبة للكثير يظهر الأشخاص على الطرف الآخر كأنّهم شخصيات في لعبة ضمن الكمبيوتر، وهذا يؤدي لدى البعض إلى تجاهل حقيقة أن الأشخاص على الطرف الآخر يمكن أن يسببوا لهم الأذى وتجعل الأمر بسيطا أن يقوم الآخرون بالأذى والسرقة وهذه الجرائم لا تعتبر حقيقية بالنسبة لهم، فهذه الأخيرة تتسّم بسمات مخصوصة عن غيرها من الجرائم، بشكل عام القدرة على الوصول لهدف معيّن بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية، وسنعرض فيما يلي السمات المميزة لهذه الجرائم وكذا وسائل الحماية التي تجنبنا الوقوع في مخاطرها.

المطلب الأول : "السمات المميزة لجرائم المعلوماتية عن غيرها من الجرائم"

الجرائم المعلوماتية طائفة من الجرائم تتسّم بسمات مخصوصة عن غيرها من الجرائم، فهي تستهدف معنويات وليس ماديات محسوسة (المعلومات)، كما أنّها تتسّم بالخطورة البالغة نظرا لأغراضها المتعدّدة، و نظرا لحجم الخسائر الناجمة عنها قياسا بالجرائم التقليدية، ونظرا لارتكابها من بين فئات متعدّدة تجعل من التنبؤ بالمشتبه بهم أمرا صعبا. ونظرا لأنها بذاتها تنطوي على سلوكيات غير مألوفة وبما أتاحته من تسهيل ارتكاب الجرائم الأخرى تمثل إيجاد وسائل تجعل ملاحقة الجرائم التقليدية أمرا صعبا متى ما ارتكبت باستخدام الكمبيوتر.

إن التحقيق والتحري في الجرائم المعلوماتية والمقاضاة تنطوي على مشكلات وتحدّيات إدارية وقانونية تتصل ابتدءا بمعيقات ومتطلبات و عمليات ملاحقة الجناة، فإن تحققت الملاحقة أصبحت الإدانة صعبة لسهولة إتلاف الأدلة من قبل الجناة أو لصعوبة الوصول إلى الأدلة أو لغياب الاعتراف القانوني بطبيعة الأدلة المتعلقة بهده الجرائم. و نظرا لأنها جرائم لا تحدها حدود و تعد من الجرائم العابرة للحدود، فتثير لذلك تحديات و معيقات في حقل الاختصاص القضائي و القانون الواجب التطبيق و متطلبات التحقيق و الملاحقة و الضبط و التفتيش.

الفرع الأول : "مجال الجريمة المعلوماتية"

إن الجريمة المعلوماتية قد ترتكب عن طريق حاسب ألي في دولة ما، في حين يتحقق الفعل الإجرامي في دولة أخرى "1".

فجرائم المعلوماتية لا تحدها حدود و تتميز بالتباعد الجغرافي بين الفاعل و المجني عليه، ومن الوجهة التقنية بين الحاسوب (أداة الجريمة) و بين المعطيات والبيانات (محلّ الجريمة) في نظام الحاسوب المستهدفة بالاعتداء، هذا التباعد قد يكون ضمن دائرة الحدود الوطنية للدولة، لكنه

و بفعل سيادة تقنيات شبكات النظم و المعلومات، امتد خارج هذه الحدود، دون تغيير في الاحتياجات التقنية، ليطال دولة أخرى يتواجد فيها نظام الحاسوب المخزنة فيه المعطيات محّل الاعتداء.

1- الأستاذ (Ubrich seiber)، جرائم الحاسب الآلي و الجرائم الأخرى المرتبطة بالتقنيات الحديثة لوسائل الاتصال، ترجمة الدكتور سامي الشوا، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، 25-28 أكتوبر 1993، و الورقة المذكورة بذاتها من أوراق التحضير للمؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات، البرازيل 4-9 جويلية 1994، ص 08.

والحقيقة أن مسألة التباعد الجغرافي بين الفعل وتحقق النتيجة من أكثر المسائل التي تثير إشكالات في مجال جرائم المعلوماتية وبشكل خاص الإجراءات الجنائية والاختصاص والقانون الواجب التطبيق، وهذا بدوره عامل رئيسي في نماء دعوات تظافر الجهود الدولية لمكافحة هذه الجرائم، ولعل هذه السمة تذكرنا بإرهاصات جرائم المخدرات و الاتجار بالرقيق وغيرها من الجرائم التي وقف تباين الدول و اختلاف مستويات الحماية الجنائية فيها حائلا دون نجاعة أساليب مكافحتها، فلم يكن من بد غير الدخول في سلسلة اتفاقيات ومعاهدات دولية لمكافحة هذه الجرائم، وذات الأمر يقال الآن بشأن أنشطة غسل الأموال، وهي في ذات الوقت الأسباب ذاتها التي تجعل موضوع جرائم الإرهاب و الجرائم المنظمة والجرائم الاقتصادية المواضيع الرئيسية على الساحة الدولية ."**1**"

<u>الفرع الثاني</u> : " الحلول المقترحة لمواجهة الجريمة المعلوماتية "

لمواجهة الجريمة المعلوماتية العابرة للحدود مواجهة فعالة، يجب تجريم صورها في القانون الوطني للمعاقبة عليها، وإن يكون هناك تعاون وتضامن دولي لمواجهة مشاكلها من حيث مكان وقوعها و اختصاص المحاكم بها وجمع المعلومات و التحريّات عنها والتنسيق بين الدول في المعاقبة عليها وتحديد صورها وقواعد التسليم فيها وإيجاد الحلول لمشكلاتها الأساسية وأبرزها:

1- يقول الأستاذ محي الدين عوض: إن الجريمة الجريمة المعلوماتية لا تعترف بالحدود بين الدول والقارّات، إذ يكفي أن نتصور أن القائم على الكمبيوتر في طوكيو يستطيع أن يحول مبلغا من المال من هناك إلى نيويورك أو مونتيريال مضيفا إليه صفرا أو بضعة أصفار، كذلك يستطيع من يعرف كلمة السرّ أن يفعل الأمر نفسه بتغيير المعلومات في الشبكة الأوروبية التي يتصل بها من أقصى الشرق عن طريق التداخل فيها.... إن السمة الغالبة للكثير من جرائم المعلوماتية، هي أنها من النوع العابر للحدود (Transnational) وبالتالي تثير من المشاكل ما تثيره أمثال تلك الجرائم كجرائم الاتجّار بالمخدرات و الاتجار غير المشروع في الأسلحة والاتجار في الرقيق الأبيض و الجرائم الاقتصادية و المالية وجرائم التلوث البيئي ...إلخ. أنظر، الأستاذ الدكتور محمد محي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 25-28 أكتوبر 1993، ص6.

1. غياب مفهوم متفق عليه بين الدول- حتى الآن- حول نماذج النشاط المكون للجريمة المتعلقة بالمعلومتية و الأنترنيت .

2. غياب الاتفاق حول التعريف القانوني للنشاط الاجرامي المتعلق بهذا النوع من الاجرام.

3. نقص الخبرة لدى الشرطة وجهات الادعاء و القضاء في هذا المجال لتمحيص عناصر الجريمة إن وجدت وجمع المعلومات و الأدلة عنها للإدانة فيها.

4. عدم كفاءة وملاءمة السلطات التي ينص عليها القانون بالنسبة للتحري و اختراق نظم المعلوماتية، لأنها عادة متعلقة بالضبط و التحري بالنسبة لوقائع مادية هي الجرائم التقليدية وغير متوائمة مع غير (الماديات) كاختراق المعلومات المبرمجة وتغييرها في الكمبيوتر.

5. عدم التناسب بين قوانين الاجرءات الجنائية للدول المختلفة فيما يتعلق بالتحري في الجرائم المتعلقة بالمعلوماتية .

6. السمة الغالبة للكثير من جرائم المعلوماتي هي أنها، من النوع العابر للحدود Transnational وبالتالي تثير من المشاكل ما تثيره أمثال تلك الجرائم كجرائم الاتجار بالمخدرات و الاتجار غير المشروع في الأسلحة و الاتجار في الرقيق الأبيض والجرائم الاقتصادية والمالية والتلوث البيئي.

7. عدم وجود معاهادات للتسليم أو للمعاونة الثنائية أو الجماعية بين الدول تسمح بالتعاون الدولي أو عدم كفايتها إن كانت موجودة لمواجهة المتطلبات الخاصة لجرائم المعلومات وسرعة التحريات فيها للكفالة بها .

ويمثل مشروع الاتفاقية الأوروبية لجرائم المعلوماتية في الوقت الحاضر المشروع الأكثر نضج لمواجهة جرائم المعلوماتية بل وواحدا من أهم أدوات التعاون الدولي في هذا الحقل.
وعوضا عن هذه المشكلات، فإننا نرى أن من أبرز المشاكل التي تواجه سياسات مكافحة الجرائم المعلوماتية لا على الصعيد الدولي بل وفي نطاق التشريعات الوطنية، عدم التعامل معها كوحدة واحدة في إيطار الحماية الجنائية للمعلومات .

إذن من تواجد استجابات قانونية حديثة للتحديات الحالية لمجتمع المعلومات بل و أكثــر مــن ذلك، فمن الضروري أن نخلق فقها جديدا من أجل الحماية الجنائية للمعلومات.

المطلب الثاني: "وسائل الحماية من الجريمة المعلوماتية"

مع التطور المستمر لطرق وأساليب الاختراق، كان لزاما أن تتطور في مقابلها وسائل وطرق للحماية، ولأهمية هذا الموضوع بالنسبة للمسؤولين عن الأنظمة و المزودات فقد كان الاهتمام بأمن وحماية المزودات من المخاطر الأمنية كبير جدّا و لا تخلوا اليوم شركة من قسم يختص بأمن وسلامة المعلومات.

ولكن في المقابل عندما نتحدث عن حماية الأجهزة الشخصية personel-Computer نجد بأن هناك قصورا كبيرا من المستخدمين لحماية أجهزتهم، فعامل الحماية عامل أساسي علــى كــل المستخدمين إدراكه.

الفرع الأوّل : "الأوامر الأساسية لأمن الأنترنيت"

أولا : "كلمة المرور"

ضمن الأنترنيت تعتبر كلمات المرور مفاتيح حياتك، فأيّ شخص يمتلك كلمة المرور الخاصة بك يمكنه أن يمتلك تماما باستخدام خدمتك مع مزود الخدمة المسجل معه و الدخول لكل مواقع الأنترنيت المختلفة ويمكنه بذلك:

- قراءة بريديك الالكتروني.
- ارسال بريد إلكتروني باسمك.
- نشر الموضوعات بساحات الحوار الالكترونية باسمك.
- شراء الأشياء ضمن الأنترنت إذا كان لديك حساب ضمن موقع تسوق او كان لديك حساب ضمن خدمة الانترنت.

لذا قبل اتخاذ أي إجراء إحتياطي تأكّد أوّلا أنّ كلمة المرور التي تخصك لم تسرق بعد، إن كنت قد اشتركت مع مزود الخدمة بالساعات، فراقب عدد ساعاتك، حيث يوفر لك مزود الخدمة بارومتر لعدد الساعات المتبقية من رصيدك ضمن موقعه، راقب عدد الساعات المتبقية في رصيدك قبل خروجك من الأنترنيت ثم راقبها من جديد عند دخولك التالي، فإن رأيت بأن هناك فرق شاسع بين آخر قراءة وقراءتك الحالية، فحتما هناك من يستخدم حسابك الشخصي، وبلغة أخرى تم اختراق كلمة المرور الخاصة بحسابك.

ثانيا: "تحميل الملفات"

توفر الانترنت كما هائلا من المعلومات، فالنشرات الاقتصادية وأسعار صرف العملات وأسعار الأسهم و نماذج وبيانات الجوازات و جداول الاختبارات المدرسية وكلّ ما يرتبط بها من تواريخ وبيانات وفوق كل ذلك البرامج والتطبيقات المتوفرة بشكل مجاني (وأحيانا هذه البرامج والتطبيقات المجانية تزرع بداخلها ملفات تجسسية، أو بعض الفيروسات المعلوماتية).

ثالثا: "أسرار الأنترنت بعد الخروج منها"

بالمقدار الذي يهمنا فيه تجسس شخص ما علينا عند عملنا على الأنترنت، فالتهديد الرئيسي يكون بعد الخروج من الأنترنت من الأشخاص الذين يتسللون إلى الكمبيوتر، لذلك يجب أن نهتم بالآثار التي تتركها عملية التحميل و الرسائل المحفوظة و التسجيلات التي نحتفظ بها، وهذا الاجراء ينفع الأفراد الذين يملكون خدمة مباشرة للدخول إلى الأنترنت في الشركات والذين لا يرغبون رؤسائهم أو مديروا الشبكات في معرفة تتبع المواقع التي يدخلونها.

الفرع الثاني: " وسائل الحماية "

نجد أن هناك قصورا كبيرا من المستخدمين لحماية أجهزتهم، فحماية الكمبيوتر من الاختراق وتدمير المعلومات عامل أساسي على كل المستخدمين إدراكه، هذا من جهة، ومن جهة أخرى

إنتشرت برامج الحماية و البرامج المضادة للاختراقات انتشارا كبيرا قد يصاب المستخدم بالحيرة فيما يختاره منها، خصوصا إذا ما أدركنا بأن بعض المخترقين يتجسسوا لصالح شركة مصنعة.

فالشركات تدرك اليوم بأن المستخدم العادي وفي أي بلد كان على جانب كبير من الوعي الذي يؤهله لاكتشاف الثغرات الأمنية، لذا بات من الواجب إتخاذ كل الاجراءات و التدابير اللازمة التي نقوم من خلالها بحماية أجهزتنا من مجرمي المعلوماتية، وهذا ما سنعرضه فيما يلي:

أوّلا : " تحديد مكان جهازك "

من العناصر المهمة بشكل كبير لحماية المنطقة الأمنية، المكان الذي نخصصه لجهازنا، فالناس يحدّدون مكان وضع أجهزتهم لما يوافقها، مثلا قربها من مصدر التيار الكهربئي ، فيجب أن نأخذ بحسباننا حقيقة أن أيّ شخص في مكان عملك او منزلك يمكنه رؤية ما نقوم به على جهازنا بإلقاء نظرة بسيطة وعابرة.

ثانيا : " طباعة ونسخ الرسائل الالكترونية المهمة "

تزود الطابعات فرصة مثلى لحماية المعلومات، فقيامنا بطبع المعلومات و حفظها في مكان أمين، فلو فرضنا مثلا ان أحدهم توصل إليها فإن نسبة اختراق منطقتنا الأمنية اقلّ ممّا ستكون عليه النتيجة عند تسرب معلوماتنا إلكترونيا بما فيه كلمة المرور الخاصة بنا.

ثالثا : " حذف الملفات المهمة "

كل مهمل يعتبر بلا أهمية في نظرنا، ولكنّه جزء منا و لو كانت المعلومات التي يحويها عنّا ضئيلة، لأنّها في المقابل تكون دسمة بالنسبة للآخرين وتكون الخيط الرفيع الذي سيقودهم إلى معلومات أخرى أكثر أهمية، لذا يجب التخلص من كلّ المعلومات التي حذفناها وأرسلت إلى سلة المهملات الخاصة بالكمبيوتر.

رابعا : "حماية بياناتك ونظامك عند ترك الجهاز"

معظمنا لا يحّب إغلاق جهازه عند تركه لبضعة دقائق، إنّ خطورة الاختراق تكمن هنا، فغيابنا عن الجهاز يعني دعوة مفتوحة لكلّ من هبّ و دبّ للعبث بالملفات كيفما شـــاء، خاصـــة وأنّ الحصول على المعلومات من جهاز الكمبيوتر سريعة، وبالتالي يجب إيقاف النظم بشكل مؤقت أو ما يعرف "السبات" Ecran de veille أو شاشة التوقف، كما يمكن وضع كلمة المرور به.

خامسا : " مسح الآثار الخاصة بنا من قائمة المستندات "

يجب أن نتعوّد دائما على مسح الآثار الخاصة بالمعلومات التي قمنا باســتخدامها أو الاطــلاع عليها من قائمة المستندات Mes documents لأنّها تبقى ركيزة أساسية للاختراق.

سادسا : " أخذ احتياطاتك عند إغلاق الكمبيوتر "

قبل إغلاق الكمبيوتر يجب القيام بشيئين مهمين :

- نسخ البيانات الحساسة على قرص مرن خارجي Disque externe
- حذف الملفات الأصلية من القرص الصلب Disque dur

سابعا : " عن طريق أنظمة كلمات المرور "

يتم وضع برامج كلمات المرور(Mot de passe) لحماية النظام كله أو ملفات خاصة بالنســبة للخبير أحيانا يتم كسرها و تجاوزها، وهناك نوعين من كلمات المرور التي يستطيع المستخدم استخدامها في جهازه الشخصي الغير مرتبط بالشبكات الداخلية وهما: كلمـــة مـــرور شاشـــة التوقف Ecran de veille وكلمة مرور تشغيل الكمبيوترSystème d'exploitation.

دراسة حالة

الفيروس المعلوماتي

المقدمة :

يمثل الفيروس أحد الأشياء الغامضة التي تسبب الحيرة والارتباك، وتتفاوت درجة رد الفعل حسب المستوى التقني ومدى الخبرة للفرد، والاختلاف يرجع إلى تناقض فكرة وجود الفيروس .فالأطباء يعتبرون الفيروس كائن حي يعيش ويتكاثر في وسط مساعد كالجسم البشري أي أنه وسط بيولوجي وبين الكمبيوتر ككيان مادي، فهناك من يستبعد الفكرة تماماً، وهنالك من لا يعطي الموضوع حقه من الاهتمام.

و قد بدأ ظهور أول فيروس سنة 1978م "**1**" أو قبلها بقليل (بحيث يصعب تحديد البداية بدقة) ولم تأخذ المشكلة شكلها الحالي من الخطورة إلاّ مع انتشار استخدام شبكة الانترنت ووسائل الاتصالات المعقدة، منها :البريد الإلكتروني .حيث أمكن ما لم يكن ممكناً من قبل من ناحية مدى انتشار الفيروس ومدى سرعة انتشاره.

و كان أول هجوم فيروسي سنة 1988 م و يدعى هدا الفيروس WORM MORRIS "**2**"، فألحق هدا الأخير خسائر كبيرة بأنظمة الكمبيوتر و ما تحتويه من معلومات.

1- www. majed@alsadhan.orgck

2- www.raddadi.com

تعريف الفيروس :

الفيروس هو عبارة عن برنامج أو مجموعة من رموز مبرمجة بشكل معين يتم إدخالها أوتحميلها في الكمبيوتر بدون معرفة صاحبه لتبدأ العمل ضد رغبته .وتسبب أمور غير متوقعة وأشياء ضارة وغير مرغوبة . معظم هذه البرامج أو الرموز تكون قادرة على تكرار نفسها وعمل نسخ طبق الأصل من نفسها لتبدأ في التكاثر والانتشار بالجهاز ."1"

و تطلق كلمة فيروس على الكائنات الدقيقة التي تنقل الأمراض للإنسان وتنتشر بسرعة، وبمجرد دخولها إلى جسم الإنسان تتكاثر وتفرز سمومها حتى تسبب دمار الأجهزة العضوية للجسم ومنها ما هو قاتل يسبب الموت .

أما الفيروس المعلوماتي فيدخل إلى الكمبيوتر يعمل نفس التأثيرات ونفس الأفعال، وله نفس قدرة التكاثر وربط نفسه بالبرامج حتى يسبب دمار الكمبيوتر دماراً شاملاً.

خصائص الفيروس المعلوماتي :

1- يقوم الفيروس المعلوماتي بتغيير خصائص ووظائف البرامج والملفات .

2- يقوم بإعادة إنشاء نفسه منتجاً كميات جديدة .

1-www.rayat.com

3- يختبر البرامج المطلوب إصابتها فإن كانت أصيبت من قبل لا يرجع إليها بل ينتقل إلى برامج أخرى وملفات جديدة .

4- البرامج المصابة قد تظل تعمل مدة طويلة بدون ظهور أي أعراض عليها .

5- يتشبه بالبرامج حتى لا يقوم أي مضاد للفيروسات باكتشافه .

ومن خلال كل هدا يتضح لماذا سمي الفيروس بهذا الاسم رغم أنه في الواقع ليس سوى برنامج من برامج الكمبيوتر .

- فالفيروس إذا عبارة عن كود برمجي (شفرة) الغرض منها إحداث أكبر قدر من الضرر؛ ولتنفيذ ذلك يتم إعطاؤه القدرة على ربط نفسه بالبرامج الأخرى عن طريق التوالد والانتشار بين برامج الحاسب وكذلك مواقع مختلفة من الذاكرة حتى يحقق أهدافه التدميرية ."**1**"

و من خلال هذا يتضح لنا جليا أن الفيروس لا يستطيع أن يعمل بمفرده دون وسط ناقل .

1-www.neelwafurat.com

الدور التدميري للفيروس :

فهو برنامج يمكن أن يصيب برامج أخرى ويقوم بتعديلها لتكون محتوية على نسخة من نفس الفيروس .إن جميع الفيروسات تنسخ نفسها، و تختفي بالكمبيوتر لكي لا يتم اكتشافها إما بطريقة ترميزها أوبأن تغير من نفسها بعض الشيء في كل مرة تتزايد بها .

إن عمل الفيروس بسيط يستطيع أن يعمل نسخ مكررة من نفسه وتنتشر بشكل تلقائي .ومع ذلك فإنه حتى هذا الفيروس البسيط يعتبر خطيرا بسبب أنه سيقوم سريعا باستعمال جميع مساحة الذاكرة المتوفرة في الكمبيوتر ويجعله في النهاية غير قادر على العمل.

الفيروس الأخطر من هذا هو النوع القادر على أن ينشر نفسه عبر الشبكات ويستطيع المرور عبر أنظمة الحماية .يمكن للفيروس أن يرسل عبر البريد الإلكتروني كملحق معه، أو عند تنزيل برامج أو ملفات مبرمجة من مواقع أخرى، أو مع قرص مدمج أو لين ، وفي أغلب الأحيان فإن مصدر هذه الملفات أو الأقراص أناس لم يقصدوا أو ينتبهوا لتواجد الفيروس .

عند الإصابة بالفيروس تبدأ رموزها بالعمل فورا، وهناك من الفيروسات من تبقى نائمة حتى تحين الظروف المناسبة لانتشارها بالكمبيوتر .

أنواع الفيروسات :

عموما هناك ثلاثة أصناف رئيسية للفيروسات :

1- فيروسات ملفات التلويث : File infector viruses

هذه الفيروسات تلحق نفسها لبرنامج الملفات ، وعادة تختار ملفات **EXE**أو**COM**، والبعض يمكن أن يصيب أي برنامج حيث يتطلب فيه ملف تنفيذ بما في ذلك ملفات **SYS**، **OV**، **PRG** و **MNU**.عندما يتم تحميل البرنامج فإنه يتم تحميل الفيروس أيضا .هناك ملفات تلويث أخرى تصل كبرامج كاملة أو نصوص مرسلة كملحق للبريد الإلكتروني.

2- الفيروسات التي تصيب نظام التشغيل Systemأو بدء العمل Boot-record:

هذه الفيروسات تصيب الرموز التي يمكنها القيام بالتنفيذ والموجودة في مناطق معينة على نظام التشغيل في القرص وفي نظام بدء العمل .تقوم هذه الفيروسات بالإلتحاق بنظام التشغيل **DOS** في القرص الصلب .العادة أن يصل قرص لين من مصدر ما ويكون محتويا على فيروس بدء التشغيل، وعندما يقوم نظام التشغيل بالكمبيوتر في العمل فإن ملفات على القرص اللين يتم قراءتها دون المساس بفيروس بدء تشغيل القرص، وإذا ما ترك القرص في جهاز تشغيله بالكمبيوتر ثم اوقف التشغيل أو أعيد تحميل برنامج نظام التشغيل فإن الكمبيوتر سينظر أولا في في جهاز تشغيل القرص اللين**A drive**، ويجد هذا القرص مع فيروس بدء التشغيل، ثم يقوم بتحميله بالقرص الصلب مما يجعل من المستحيل استعمال هذا القرص لفترة من الوقت حتى معالجة الأمر ويحتاج لذلك أن يكون لدينا قرص بدء تشغيل لين للكمبيوتر .

3- الفيروسات الصغيرة: Macro viruses

تعتبر ضمن أغلب الفيروسات الشائعة، وتقوم عادة بعمل أقل أضرار الفيروسات .تقوم هذه الفيروسات بإصابة برنامج معالجة الكلمات **MICROSOFT** و**WORD** وتطبيقاته حيث تقوم بإدخال كلمات وفقرات جمل غير مرغوبة، كذلك من الممكن أن تقوم بإصابة ملفات مستندات النصوص النشطة **HTML**المحتوية على نصوص **JAVA** أو الأنواع الأخرى من الرموز التنفيذية وتقوم بالتالي بنشر الفيروس.

4- الفيروس المتعدد الاجزاء: Multipartite Virus

و هو الذي يقوم باصابة الملفات مع قطاع الاقلاع في نفس الوقت و يكون مدمراً في كثير من الاحيان اذا لم تتم الوقاية منه .

5- الفيروس المتطور : Polymorphic Virus

هي فيروسات متطورة نوعا ما حيث انها تغير الشفرة كلما انتقلت من جهاز الى آخر .نظريا، يصعب على مضادات الفيروسات التخلص منها لكن عمليا و مع تطور المضادات فالخطر اصبح غير مخيف .

6- الفيروس المختفي : Stealth Virus

تخفي نفسها بان تجعل الملف المصاب سليما و تخدع مضادات الفيروسات بان الملف سليم و ليس مصاباً بفيروس .مع تطور مضادات الفيروسات اصبح من السهل كشف هذا النوع .

يجب أن يجري العمل التنفيذي على رموز الفيروس كي يكون لها أي أثـر أو فعـل، ولهـذا فـإن الملفات التي يعاملها الكمبيوتر على أنها مجرد معلومات نقية يمكن اعتبارها ملفات آمنـة .يتضـمن ذلك ملفات الجرافيك كالصور وكذلك ملفات الصوت مثل **gif**و **jpg**و **mp3**و **wav**.إلخ .يضاف لهذا الملفات المحتوية على نصوص فقط مثل **.txt**.وبالتالي فـإن رؤيتـك لصـورة لـن يصـيب كمبيوترك بالفيروس .إن رمز الفيروس يجب أن يكون بشكل تركيبة **form**، مثل تركيبـة ملفـات البرامج **exe**.أو تركيبة ملفات معالجة الكلمات **doc**.والتي يجب على الكمبيوتر أن يقوم بـإجراء العمل التنفيذي عليها."**1**"

كيف تعمل الفيروسات ؟

في الواقع يقوم الفيروس في حالة إصابة الملف بإضافة نفسه في بداية أو نهاية الملف المصاب، دون أن يقوم فعلياً بأي تغيير في مكوّنات الملف الأصلية، فنلاحظ أنه عند استدعاء البرنامج فإنه يعمل بشكل طبيعي.

والآن لنتصوّر أنه تم اصابة البرنامج بفيروس، في الواقع يقوم الفيروس بلصق نفسه في البرنامج كما أسلفنا دون أن يغير في محتويات الملف شيئاً، و طريقة اللصق تكون، إما أنه يقوم بلصق نفسه في بداية البرنامج، بحيث يتم تشغيله هو قبل البرنامج نفسه.

1- د.حسام شوقي، حماية و أمن المعلومات على الأنترنت، الطبعة الأولى، دار الكتب العلمية، 2002 ، ص 17.

وقد تكون طريقة التحاق الفيروس بالملف بأن يضع نفسه في نهاية البرنامج المصاب .و يضع علامة في بدايته، إن هذا الفيروس، يختبئ في نهاية الملف المصاب، و يضع في مقدّمة البرنامج مؤشّراً بحيث أنه عندما يتم استدعاء البرنامج و تشغيله، يحوّل السيطرة للفيروس بدلاً من تشغيل البرنامج .

وفي الحالتين قد يعود الفيروس بعد الانتهاء من تنفيذ عمله المؤذي لتشغيل البرنامج، و لكنه قد لا يعود أيضاً، و يسبب أضراراً جسيمة للجهاز .

علامات وجود فيروس في الجهاز :

- ✓بطء الجهاز الشديد، بما لا يتناسب مع عدد البرامج التي تعمل في نفس الوقت .
- ✓امتلاء القرص بما لا يتناسب مع عدد و حجم الملفات الموجودة عليه .
- ✓ظهور مربّعات حوار غريبة اثناء العمل على الجهاز .
- ✓اضاءة لمبة القرص الصلب أو القرص المرن، دون أن تقوم بعملية فتح أو حفظ ملف.

لابد أن تعرف أن هذه العلامات لا تعني بالضرورة وجود فيروس، فقد يكون بعضها بسبب مشكلة في عتاد الجهاز مثلاً .

مميزات الفيروسات :

1- القدرة على التخفي :

للفيروسات قدرة عجيبة على التخفي والخداع عن طريق الإرتباط ببرامج أخرى .كما تم أيضاً تزويد الفيروسات بخاصية التوميه والتشبّه .حيث أن الفيروس يرتبط ببرنامج يقوم بعرض أشياء مثيرة، وعند بداية تشغيله يدخل إلى النظام ويعمل على تخريبه .

وللفيروسات عدة وسائل للتخفي منها ارتباطه بالبرامج المحببة إلى المستخدمين ..ومنها ما يدخل النظام على شكل ملفات مخفية بحيث لا تستطيع ملاحظة وجوده عن طريق عرض ملفات البرنامج، وبعض الفيروسات تقوم بالتخفي في أماكن خاصة مثل ساعة الحاسب وتنتظر وقت التنفيذ .
كما أن بعضها تقوم بإخفاء أي أثر لها حتى أن بعض مضادات الفيروسات لا تستطيع ملاحظة وجودها ثم تقوم بنسخ نفسها إلى البرامج بخفة وسرية.

2- سرعة الإنتشـــــار :

يتميز الفيروس أيضاً بقدرة هائلة على الإنتشار، وقد سبق وأن قدمت العوامل التي تساعده في ذلك. فعندما نقوم بتشغيل الملف المصاب ليبدا في التكاثر و يبدأ الفيروس بالعمل، و كلما قمنا بفتح ملف ما إلا و انتشر الفيروس بداخله، و مع اتساع شبكة الأنترنت عبر أنحاء العالم فإن سرعة انتشار هدا الأخير تضاهي سرعة الكمبيوتر و سرعة بعث و استقبال المعلومات في أن واحد.

3- **القدرة التدميرية :**

تظهر عندما يجد الفيروس المفجر الذي يبعثه على العمل كأن يكون تاريخ معين' كفيروس تشرنوبل' فيقوم الفيروس بتدمير البيانات الموجودة على الجهاز فهي تعتبر الهدف المعتاد لأي فيروس وتعتبر فيروسات الماكرو التى تصيب برامج مثل word وExcel من اكثر انواع الفيروسات ايذاءا لانها تعبث بالبيانات الشخصية للمستخدم كما قد يؤدي ايضا الى عدم استقرار النظام وكثرة ظهور رسائل بدل المعلومات المخزنة بالكمبيوتر.

استراتيجية هجوم الفيروس و أماكنه الإستقرارية :

أهداف هامة يجب عليه أن ينجزها وهي إمّا أن تكون برنامج أو ملف معين،وهدف الهجوم يختلف من فيروس إلى آخر وأيضاً حسب نظام التشغيل فيبحث الفيروس عن أهداف يضمن وجودها في أي نظام تشغيل، وهي التي لا يستطيع أي نظام أن يعمل بدونها .

وفي نظام ويندوز أو أي إصدار من أي نظام تشغيل آخر يعتمد على DOSفإن الملف المستهدف دائماً من قبل الفيروسات هو COMMAND.COM وذلك لأن الملف موجود دائماً في الدليل الرئيسي للفهرس الخاص بالنظام، وحيث أن هذا الملف هو المسؤول عن استقبال أوامر التشغيل التي تدخلها وتقرير تنفيذها إن كانت من أوامر التشغيل الداخلية أو من أوامر التشغيل الأخرى التي تنتهي بالامتدادات COM, EXE, BAT.

وهناك حيلة يلجأ إليها بعض المبرمجين الأذكياء وهي أن يغير اسم هذا الملف لكي يصعب على الفيروس ربط نفسه به .

,هناك أيضا ملفات (SYS, CONFIG, BAT, AUTOEXEC)لأن النظام يبحث عن هذه الملفات عند بدء التشغيل، وينفذ ما بها من تعليمات . وهناك ملفات أخرى تمثل إغراء أكثر جاذبية للفيروس وهي (IBMBIO.COM, IBMDOS.COM) :وذلك لأنها ملفات مخفية، فبالرغم من وجودها في الفهرس الرئيسي إلاّ أنه يصعب اكتشاف الفيروس عند عرض دليل الملفات .

ومن أماكن الفيروسات المفضلة مخزن CMOS وهو مكان في الذاكرة يتم عن طريقه ضبط ساعة النظام ."1" وهذا المكان في منتهى الخطورة لأنه:

أولاً /توجد به طاقة عن طريق البطاريات التي تستخدم في المحافظة على توقيت النظام حتى بعد أن يتم إغلاق الكمبيوتر.

وثانياً /لأنها أول مكان يتم تشغيله عند بدء التشغيل، كما أن هذا المكان لا يظهر عند عرض الملفات بالأمر DIR أيضاً عن طريق هذا المكان يحدد الفيروس توقيت تشغيله.

العوامل التي أدت إلى سرعة انتشار الفيروسات :

1- التوافقية: (Compatibility)

وتعني قدرة البرنامج الواحد على أن يعمل على حاسبات مختلفة وعلى أنواع وإصدارات مختلفة من نظم التشغيل،وهذا العامل رغم تأثيره الإيجابي والهام بالنسبة لتطوير الحاسبات إلاّ أن أثره كان كبيراً في سرعة انتشار الفيروسات كما ساعدت أيضاً البرامج المقرصنة في سرعة انتقال الفيروسات."2"

1- وجها لوجه الهاكرز بلا أقنعة، الطبعة الأولى، 2003، شعاع للنشر و العلوم (ترجمة و تحقيق: د.مأمومن نعيم)

2- د.حسام شوقي، السابق، ص22.

2- وسائل الإتصالات: (Communications)

كان لوسائل الاتصالات الحديثة السريعة دور هام في نقل الفيروسات، ومن أهم هذه الوسائل : الشبكات بما فيها شبكة الانترنت وإلاّ لما استطاع فيروس الحب I LOVE YOU أن يضرب أجهزة في أمريكا وهو مصدره الفلبين ."1"

3- وسائط التخزين :

مثل :الأقراص المرنة Floppyوالأقراص المضغوطة CDوخاصة إذا كانت صادرة عن جهاز مصاب بالفيروس، فإن قدرته على التنقل بسرعة تجعل انتشاره سهل و بسيط جدا.

الحماية من الفيروسات :

للحيطة و الحذر من الفيروسات-خاصة إذا كنت معتاداً على تبادل الأقراص المرنة، أو الملفات عبر الانترنت -لابد من اتخاذ الخطوات التالية :

✓لابد من وجود برنامج الحماية من الفيروسات في جهاز الكمبيوتر .

✓لابد أن تقوم بتحديث برنلمج الحماية من الفيروسات بشكل دوري، وإلا فلا فائدة من وجوده .

✓لا تقم بفتح المرفقات في أي E-MAIL لا تعرف مرسله .

✓لا تقم بفتح المرفقات في E-MAIL إذا وجدتها تنتهي بـــ exeأو batأو أي امتداد لا تعرفه .

1- www.raddadi.com

✓افحص الملفات ببرنامج الحماية قبل أن تقوم بفتحها.

✓احرص على فحص جميع البرامج التي تقوم بتنزيلها من الإنترنت، أو تشغيلها من قرص مرن أو CD قبل أن تشغّلها.

✓داوم على زيارة المواقع التي تهتم بالحماية من الفيروسات، للإطلاع على كل ما هو جديد في هذا المجال .

برامج الحماية :

كما أسلفنا لابد من وجود برنامج الحماية من الفيروسات في الجهاز، ويقوم البرنامج بفحص وتدقيق الملفات و حماية الجهاز كما ينبغي وهو يقوم بهذا العمل عن طريق البحث عن بصمات الفيروسات فلكل فيروس بصمة عبارة عن رقم محدد و برنامج الحماية في الواقع يبحث عن هذه البصمة المحددة فإن وجدها فإنه يعلن عن وجود الفيروس. خاصة أن الكثير من الفيروسات تتم كتابتها ونشرها في الأسبوع الواحد، فمن المهم جداً أن يكون برنامج الحماية من الفيروسات محدّثاً باستمرار. و لعل أشهر برامج مكافحة الفيروسات (أو الحماية من الفيروسات) اثنين، هما برنامج Nortonللحماية من الفيروسات ، و برنامج McAffee.

دراسة فيروس : " بلاستر"

ولادة فكرة مدمرة :

الأربعاء 16 جويلية 2003، الساعة 11:00 GMT مساء بتوقيت واشنطن: ثغرة أمنية جديدة تعلن MICROSOFT عن اكتشافها في أنظمة WINDOWS 2000 وXPوNT4، وServer 2003، وتحديداً في طريقة تعامل أنظمة التشغيل مع بروتوكول "استدعاء الإجراءات عن بعد Remote Procedure Call, RPC أطلقت MICROSOFT رقعة برمجية لتأمين أنظمة التشغيل المعرضة للخطر، وهي في هذه الحالة مئات الملايين من أنظمة التشغيل المنتشرة حول العالم، خاصة في بيئات الأعمال، واصفة الثغرة الأمنية المكتشفة بالخطيرة، والتركيز على الضرورة "الطارئة" لتركيب الرقعة، نتيجة سهولة استغلال هذه الثغرة لتشغيل شيفرات برمجية عن بعد على أنظمة WINDOWS التي تتضمنها، إذا ما رغب مخترق في ذلك. "**1**"

الخطر المرتقب :

الخميس 17 جويلية، 10:00 GMT صباحاً: أدرك محللو أمن المعلومات الخطر، فرفعت شركات مكافحة الفيروسات وشركات أمن المعلومات من مستوى مؤشرات الأخطار الأمنية، وأطلقت تحليلات وتحذيرات تنبئ بأخطار هذه الثغرة بالغة الانتشار. ونصح المحللون جميع مديري الأنظمة ومستخدمي إصدارات WINDOWS 2000 وXPوNT4 وServer 2003 بالمسارعة إلى تركيب الرقعة الأمنية التي أطلقتها MICROSOFT لمعالجة المشكلة."**2**"

1– www.ayna.com

2– www.securityresponse.com

ونتيجة لذلك رفعت شركة ISS لأمن المعلومات مؤشر AlertCon إلى المستوى 2، وهو مؤشر يدل على مستوى التهديد الأمني الحالي للمعلومات عبر الإنترنت.

إغراءات الثغرات الأمنية :

الجمعة 18 جويلية، GMT 9:30 صباحاً: معهد SANS الشهير لأمن المعلومات يؤكد أنباء ترددت في الإنترنت عن ثغرة أمنية اكتشفت في جميع إصدارات أنظمة تشغيل Cisco IOS وروترات شركة سيسكو، الأمر الذي يعرض معظم شبكات الحواسيب حول العالم لخطر هجمات حجب الخدمة (DoS). ويؤكد المعهد كذلك، اكتشاف ثغرة أمنية أخرى في بروتوكول RPC، لكن في أنظمة تشغيل UNIX هذه المرة.

السبت 19 جويلية: يتابع محاولاته لليوم الثالث على التوالي، لاستغلال ثغرة RPC لاختراق المزود. وفجأة.. يكتشف أنه قد يكون من الأسهل كتابة برنامج يستغل هذه الثغرة من داخل المزود، ثم أن يرسله إليه بطريقة معينة. "[1]" كفيروس مثلاً!

الأحد 20 جويلية: تمكن من تحقيق فتح مهم، فقد تمكن من الإرسال عبر المنفذ رقم 135 لبروتوكول TCP، لتصل إلى مستمع بروتوكول RPC الموجود على عدة مزودات، ثم تمكن من ربط هذه المزودات حصراً مع جهازه، وإرسال طلب تشغيل حسب النموذج الكائني الموزع

1- www.ayna.com

للمكونات DCOM، الذي يتضمن ثغرة في بنيته البرمجية قد تسمح بفيضان ذاكرة الشيفرة البرمجية الوسيطة (buffer overflow) عند استقبال رسالة محددة عبر المنفذ 135."1" ما قد يتيح تنفيذ شيفرة برمجية مرفقة في الطلب المرسل عن بعد، عوضاً عن الشيفرة البرمجية الأصلية للبرنامج، الأمر الذي قد يسمح له بإرسال برنامج لاختراق المزود!

بوادر الخطر :

الاثنين 21 جويلية، 9:00 GMT صباحاً: يبدو أنه ليس وحيداً في محاولات استغلال ثغرة RPC، فقد أرسلت مجموعة أمنية تسمى LSD لشركات أمن المعلومات شيفرات برمجية تجريبية أنتجتها، ونجحت من خلالها في اختراق أجهزة WINDOWS مختلفة، وذلك اعتماداً على ثغرة RPC.

الساعة 11:00 GMT صباحاً: شركة ISS ترفع مؤشر AlertCon لأمن المعلومات إلى المستوى 3، الأمر الذي يعني وجود هجمات مركزة متعددة عبر الإنترنت، وذلك نتيجة ورود تقارير للشركة عن محاولات لاستغلال ثغرة بروتوكول RPC في أنظمة WINDOWS، وثغرة روترات سيسكو لاختراق مواقع وحواسيب عبر الإنترنت."2" وتطلق الشركة تحذيرات شديدة إلى مديري الأنظمة وعموم المستخدمين لسد هذه الثغرات في شبكاتهم بأسرع ما يمكن.

1- www.symantec.com

2- www.securityresponse.com

الساعة GMT 6:00 مساء: الارتباك يصيب الكثير من مديري الشبكات، الذين يصلون الليل بالنهار للإسراع في سد الثغرة في جميع الأنظمة المرتبطة مع شبكاتهم، وسد منافذ بروتوكول TCP رقم 135 و139 بشكل رئيسي."**1**"

تحذيرات أكاديمية :

الأربعاء 23 جويلية: معهد SANS يحذر من أن عدد الأجهزة المزودة بأنظمة WINDOWS والتي تتضمن ثغرة RPC يزيد عددها بأكثر من عشرة أضعاف عن عدد الأجهزة التي كانت تعاني من الثغرة التي اعتمدت عليها دودة CodeRed الشهيرة، منذ عامين تقريباً. ويضيف تحذير المعهد أن أية دودة ستعتمد على هذه الثغرة قد تتمكن من تحقيق أضرار تفوق الأضرار التي حققتها CodeRed بأكثر من 10 مرات. كما يحذر من أن إغلاق المنفذ 135 لن يكون كافياً لمديري الشبكة."**2**"

الأحد 27 جويلية، GMT 11:00 صباحاً: شركة ISS لأمن المعلومات تحذر من أن تركيب الرقعة فقط لا يحمي المزودات والأجهزة من الثغرة، بل يجب إعادة تشغيل الأجهزة يدوياً، لتفعيل ملفاتها، وذلك عقب اختبار مزودات تم تركيب الرقعة عليها دون أثر."**3**"

1- www.ayna.com

2- www.securityresponse.com

3- نفس المرجع الأول.

الخميس 31 جويلية، GMT 10:00 صباحا: مركز "فريق الاستجابة لطوارئ الحواسيب" (CERT/CC) الشهير في مجال أمن المعلومات، والتابع لجامعة Carnegie Mellon الأمريكية يطلق تعميماً يشدد على ضرورة الإسراع بتركيب الرقعة الأمنية وإيقاف عمل كثير من الخدمات وإغلاق منافذ عديدة على جميع الأجهزة في البلاد، كما ينصح جميع المستخدمين بتركيب جدران نارية.

الجمعة 1 أوت، GMT 9:00 صباحاً: قسم "تحليل المعلومات وحماية البنية التحتية القومية لتقنية المعلومات" التابع لوزارة الأمن الوطني الأمريكية تطلق تحذيراً عاماً للشركات والمواطنين ينذر بخطر قد يؤثر بشدة على شبكة الإنترنت، نتيجة استغلال ثغرة RPC. وتشير إلى ازدياد كبير في عمليات سبر منافذ الأجهزة عبر الإنترنت، بحثاً عن الثغرة. ويؤكد التعميم الذي أصدرته الوزارة أن عدة طرق ناجحة قد اكتشفت عبر الإنترنت، لاستغلال ثغرة RPC لاختراق الأجهزة و"التحكم بها بشكل كامل"."**1**"

<u>استغلال الثغرة الأمنية RPC</u> :

الاثنين 4 أوت: ظهور أداة برمجية لاختراق أنظمة WINDOWS التي تتضمن ثغرة RPC من خلال شبكات الدردشة IRC. وشركة Symantec تعلن بداية عن ظهور دودة تعتمد على ثغرة RPC، ثم تصحح إعلاناها إلى وجود أداة برمجية للاختراق وليست دودة!"**2**"

1- www.ayna.com

2- www.securityresponse.com

الجمعة 8 أوت: تحمس المخترق لفكرة تعطيل موقع MICROSOFT، وينهي كتابة دودة تعتمد على ثغرة RPC، ويُضمّن فيها شيفرة برمجية للهجوم على موقع windowsupdate.com التابع MICROSOFT، والذي يتضمن الرقعة الأمنية التي تسد ثغرة RPC، وذلك في الفترة بين 15 أوت و31 ديسمبر، في محاولة لمنع الأجهزة المصابة من تنزيل الرقعة.

السبت 9 أوت: يؤمن عدة مزودات تشغل بروتوكل TFTP (Trivial FTP)، ويضع شيفرته البرمجية المدمرة ضمن ملف msblast.exe الخاص بنظام WINDOWS 2000 على بعضها، والخاص بنظامWINDOWS XP على بعضها الآخر، ليتم تحميل هذه الشيفرة منها آلياً إلى الأجهزة التي ستصيبها الدودة.

ظهور بلاستر (BLASTER) :

الأحد 10 أوت: ينهي كتابة الشيفرة البرمجية ويطلق دودته Blaster إلى فضاء الإنترنت.

الاثنين 11 أوت: بعد حوالي 25 يوماً من انطلاق الفكرة، شركات مكافحة الفيروسات تعلن عن ظهور أول دودة تعتمد على ثغرة RPC عبر الإنترنت، تحمل الاسم MSBlast أو Blaster، وتصيب أنظمة WINDOWS من خلال إرسال طلبات DCOM عبر بروتوكول RPC من خلال المنفذ 135، ثم تركب مزود TFTP على الجهاز المصاب، وتنزل شيفرة برمجية مدمرة من عدة مزودات TFTP، ثم تضيف مفتاحاً إلى سجل النظام (Registry) يسمح للدودة بتحميل ذاتها عند إعادة إقلاع الجهاز، لتبدأ في محاولة الانتشار."**1**"

1- www.symantec.com

الخميس 14 أوت، GMT 10:00 صباحاً: ظهرت دودتان جديدتان محورتان عن دودة Blaster تحت اسم Blaster.B وBlaster.C في آسيا، وظهور برنامج حصان طروادة تحت اسم RPCSpyBot وجميعها تعتمد على ثغرة بروتوكول RPC.

الأثار الأولية لظهور الفيروس :

الجمعة 15 أوت، GMT 9:00 صباحاً: MICROSOFT تنجو بأعجوبة من هجمة موزعة لحجب الخدمة كانت ستنتج عن الأجهزة المصابة بدودة Blaster، وذلك نتيجة خطأ ارتكبه في كتابة عنوان الموقع ضمن شيفرة الدودة ذاتها، ما أدى إلى توجيه الهجمات إلى عنوان غير موجود!"**1**"

الأحد 17 أوت: يقرر كتابة دودة جديدة لإصلاح الأجهزة التي أصيبت بدودة Blaster، من خلال تركيب الرقعة الأمنية اللازمة، وأن تبقى فعالة حتى شهر جانفي 2004، لضمان تنظيف كل ما تصيبه دودة Blaster.

الاثنين 18 أوت: دودة Blast.D أو Nachi تنتشر في الإنترنت، بهدف إصلاح الأجهزة التي تضررت من Blaster، وتسبب عوضاً عن ذلك، أضراراً جديدة بتخفيض سرعة الاتصال بالإنترنت، وشغل مزودات MICROSOFT."**2**"

1-www.securityresponse.com

2-www.ayna.com

الثلاثاء 19 أوت، GMT 9:00 صباحاً: ضغط صحفي كبير من صحافة تقنية المعلومات على MICROSOFT، وتحميلها ذنب كل ما حدث بسبب رداءة أسلوب ترقيع منتجاتها أمنياً. وMICROSOFT تعلن أن نظام الترقيع لا تشوبه شائبة، لكنها تعلن في الآن ذاته أنها ستبدأ اختبار نظام ترقيع أمني آلي لبرامج OFFICE ومزود SQL ابتداء من شهر سبتمبر، على أن تطرح نظاماً شبيهاً لأنظمة WINDOWS لاحقاً."**1**"

الأربعاء 20 أوت: يحاول التخلص من أية آثار تشير إلى أنه الذي كتب فيروس Blaster، ويعود إلى لعب Counter Strike مع أصدقائه!

<u>طريقة مكافحة الفيروس</u> :

يمكن التخلص من بلاستر بطرق عديدة، وقد إخترنا احدى الطرق السهلة :

فقد صمم فيروس MSBlaster أو LoveSAN، لإرسال كتل بيانات بصورة متكررة لموقع التحديثات لدى MICROSOFT وهو windowsupdate.microsoft.com.

ويصيب BLASTER الكمبيوترات التى تعمل بـــ WINDOWS XP وWINDOWS 2000 وWINDOWS NT وMICROSOFT SERVEUR 2003. ويحتاج التخلص من الفيروس التوجه لموقع تحديث MICROSOFT وتنزيل إصلاح للثغرة الموجودة في نظام WINDOWS.

1-www.securityresponse.com

حيث تظهر أعراض الإصابة بعدة أشكال منها:

- وجود ملف msblast.exe في WIDOWS SYSTEM32 DTRECTROY.

- رسائل خطأ تشير إلى وجود خلل في خدمة التحكم عن بعد RPC ، والتي تتسبب في إعادة تشغيل أو وقف البرنامج.

ويضيف البرنامج سطرا هو windows auto update"="msblast.exe لمفتاح السجل:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

ليعمل الفيروس عند إعادة تشغيل (WINDOWS) وتبين أن الفيروس قد صمم للهجوم بأسلوب الحرمان من الخدمة Denial-of-Service على موقع تحديث WINDOWS."1"

وحاول إرسال بيانات لمنفذ TCP 135، ويتوفر حل لإزالة الفيروس على الموقع:

http://www.microsoft.com/technet/tr...in/MS03-026.asp

ويمكن ازالة الفيروس بطريقة أخرى و هذا بتنزيل ملف من الموقع:

و للتحميل لابد من النقر على الرابط التالي :

http://securityresponse.symantec.co...er/FixBlast.exe

ولمن لا يوجد لديه برنامج مكافحة فيروسات فلا يوجد أي عذر مع توفر برنامج مجاني مثل اي في جي على قرص مجلة WINDOWS أو من الموقع:

.http://windowsupdate.microsoft.com

1- د.محمد حسن، حماية البرمجيات و طرق كسرها، الطبعة الأولى، دار الرضا للنشر،2004،ص11.

إلقاء القبض على مبرمج فيروس بلاستر: Blaster

تم القاء القبض على مراهق امريكي اسمه (جيفري لي) يعتقد بأنه كاتب فيروس بلاستر الذي سبب تعطل شبكة الانترنت وأدى الى اصابة ما يزيد على 500.000 جهاز في بداية ظهوره حول العالم وذلك حسب تقدير شركات امن المعلومات على الانترنت وحمايتها، كما يعد الخبراء هذا الفيروس الأسوأ خلال سنة 2003."**1**"

الفيروس عبارة عن دودة تصيب نظام windows وذلك للاصدارات NT و(2000) وxp و2003 server وكانت الاجهزة التي لم تقم بعمل تثبيت للتحديث من موقع مايكروسوفت عرضة للاصابة بهذا الفيروس. وقد سلم جيفري نفسه في الوقت الذي كانت السلطات تبحث عنه، وحضر جيفري الجلسة الأولية لمحاكمته في المحكمة.

بعض الأضرار الناجمة عن الفيروس بلاستر:

✓اصيب حوالي386000 جهاز حاسب حول العالم في بداية ظهوره بمعدل 2500جهاز في الساعة.

✓تعطل موقع microsoft و اصبح الوصول اليه صعباً و ذلك لمدة 4ساعات .

✓قال رئيس كوريا الجنوبية المنتهية ولايته كيم داي جونغ إنها مشكلة خطيرة أدت إلى تعطيل حياة المواطنين موضحا أنه طالب الحكومة باتخاذ جميع الإجراءات لمنع تكرار أي هجمات بفيروس الكمبيوتر. ولم تعط الدولة أي تقديرات عن الخسائر من الهجوم، لكن اتحاد شركات التأمين في كوريا قال إنه قد يضطر لدفع نحو مليار وون (860 ألف دولار) كتعويضات.

1– www.**aldjazeera.net**

✓انخفضت أحجام التداول في بورصة الأسهم الكورية الجنوبية إلى أدنى مستوياتها منذ 13 شهرا مع إحجام المستثمرين عن تقديم عروضهم عن طريق سماسرة الإنترنت. وارتفعت أسهم شركات أمن الإنترنت في حين هبطت أسهم شركات تقديم خدمة الإنترنت في سول وطوكيو.

✓تعطيل لعديد من المصالح الحكومية وشركات الطيران.. واضافت الاحصائية ان هناك العشرات من الاجهزة التي اصيبت من جراء هذا الفيروس، الذي تسبب ايضا في تعطيل من الشركات ومصالح الدول..

✓افاد خبراء بان الفيروس وصل إلي 69 دولة على الاقل.

✓ وطبقا للاحصائيات تعتبرالولايات المتحدة ،بريطانيا و كوريا الجنوبية الأكثر تضرراً حيث يستغرق الفيروس ثلاثين ثانية فقط للوصول ال الحواسب غير المصابة.. وعلى خلاف العديد من الفيروسات الحديثة ينتشر هذا الفيروس بنفسه ويحاول اصابة أى حاسب الى ضعيف يعمل بنظام النوافذ windows مادام متصلا بالانترنت.. ويسيطر الفيروس على الحاسب عن طريق استخدام ثغرة فى النظام الذى تستخدمه العديد من نسخ WINDOWS MICROSOFT فى نقل الملفات الانترنت.

✓ازدياد الضغط على شبكة الإنترنت، وتوقف عدد كبير من المواقع عن العمل منها مواقع شركتي السيارات BMW وجنرال موتورز، ومصرف Nordea Bank الذي أغلق 70 فرعاً من فروعه نتيجة الإصابة. وإصابة آلاف الشبكات المحلية ببطء شديد.

✓أدت إعادة تشغيل آلاف المزودات حول العالم بعد تركيب الرقعة، إلى إهدار مئات الساعات من أوقات العمل.. كثير من مديري تقنية المعلومات في الشركات يتلقون توبيخاً من رؤسائهم لإضاعة الوقت دون سبب واضح.

✓مركز CERT "**1**" يقدّر إصابة 1.4 مليون جهاز بالدودة، وآلاف أنظمة 2000windows و xp و NT4 و Server 2003 تبدأ بالانهيار كلما تم تشغيلها نتيجة محاولة الدودة تنزيل الشيفرة البرمجية المدمرة الخاصة بأنظمة xp على أجهزة تتضمن 2000windows وبالعكس، وذلك من مزودات TFTP التي أنشأها.

✓وأصيبت بعض المؤسسات الكبرى ؛ حيث ضرب الفيروس مصرف الاحتياطي الفيدرالي في أتلانتا، كما تسبب الفيروس في غلق الحواسب في إدارة تراخيص السيارات في ولاية ميريلاند الأمريكية أيضا، بالإضافة إلى مكاتب حكومية في هونج كونج

✓ كما أن الإصابة بالفيروس ألحقت خسائر تقدر بحوالي 300 مليون دولار في حسابات الوقت الضائع.

1– WWW.CERT.ORG

مركز البحث و الإحصائيات العالمي Computer emergency reponse team

الخاتمـــــــة :

الأمر الجدير بالذكر هنا، هو أن هذه الهستيريا التي سبقت ورافقت انطلاق دودة Blaster، يرجح أنها ساهمت في إنشائه وانتشاره، ومن المرجح كذلك أنها دفعت المئات أو الآلاف من الأشخاص عبر العالم إلى تجربة كتابة فيروس أو اختراق الأنظمة عبر الإنترنت عبر ثغرة RPC بدافع الفضول أو بقصد التخريب.

إلا أن هذا الزخم الأمني الذي تصاعد عبر الإنترنت، والذي لم نشهده إلا نادراً (وقت انتشار فيروس الحبI LOVE YOU ومليسا MELISSA وCodeRed ومرتين عند حدوث هجمات ضخمة موزعة لحجب الخدمة DDoS)، فتح النقاش حول ضعف نظام "ترقيع الثغرات الأمنية" الذي تتبعه شركات أنظمة التشغيل والبرمجيات، والذي يتطلب أن يقوم مئات ملايين المستخدمين بتنزيل الرقعة وتركيبها على أجهزتهم، وهو أمر يستحيل أن يتحقق بشكل كامل عبر العالم، حيث ستبقى ملايين الأجهزة بدون الرقعة الأمنية، وبالتالي يكون خطر وقوع الأضرار حتمياً.

ربما يكمن الحل في أن تُلزِم الشركات والحكومات مقدمي أنظمة التشغيل والبرمجيات في عقود الشراء بأن يؤمنوا نظام ترقيع تلقائي للمستخدمين عبر إنترنت. كما يمكن تعميم نظام "للترقيع الإجباري" بحيث تصبح مسؤولاً عن الأضرار التي قد يتسبب بها نظامك للأنظمة الأخرى، نتيجة عدم تركيبك الرقعة الأمنية على جهازك، تماماً كنظام تأمين السيارات الإجباري المعمول به في

معظم دول العالم، والذي يجبرك بطريقة أو أخرى، على دفع تكاليف إصلاح جميع السيارات التي قد تصطدم بها، إذا ما تعطلت مكابح سيارتك فجأة نتيجة إهمالك. ويُرجح بعض المحللين أن أياً من هذه الحلول قد يكون كفيلاً بتقليص آثار الفيروسات والديدان، وبالتالي الخسائر الكبيرة، بشكل ملموس، وبصورة تفوق آلية "الترقيع عند الخطر" التي ساهمت في انتشار دودة Blaster وربما نشوئها من الأساس!

الخاتمة

الخاتمــــة:

لقد تناولنا في هذا البحث المتواضع، موضوع معاصر ألا وهو الجريمة المعلوماتية وآثارها الاقتصادية، فهو بالتأكيد موضوع لا يخص الجرائم التقليدية و ليس مجرد جريمة بثـوب جديد أو بوسيلة جديّة، إنّها بحق جرائم جديدة في محتواها ونطاقها ومخاطرها، ووسـائلها، ومشاكلاتها، وفي الغالب في طبائعها وسمات مرتكبيها.

فقد قسمنا هذا البحث إلى فصلان، تناولنا في أوّلهما ماهية الجريمة المعلوماتية من خـلال تعريفها بغض النظر عن المصطلحات المستعملة للدلالة عليها، ثم تحديد طبيعتها بـالتطرق إلى تاريخ نشأتها وتطورها، وكذا موضوع الجريمة أو محلها الذي يعبر عنه بالمعلومـات والمعطيات وكذا البرامج و البيانات، ثم تطرقنا فيما بعد إلى دور الكمبيوتر فـي الجريمـة الذي قد يكون كأداة في ميدان الجريمة أو وسيلة لارتكابها وقد يكون من جهة أخرى كأداة لاكتشاف الجريمة، ثم نعرج إلى تصنيف الجريمة المعلوماتية تبعا لنوع المعطيات ومحـل الجريمة، تبعا لدور الكمبيوتر، تبعا لمساسها بالأشخاص و الأموال أو تصـنيفها كجـرائم الكمبيوتر وجرائم الأنترنت.

أما في الفصل الثاني فقد تعرضنا إلى ميكانيزمت ودوافع ارتكاب الجريمة المعلوماتية مـن خلال عرض صفات مرتكبي هذه الجريمة ودوافع ارتكابها و هذا بالتطرق إلى صفات كلّ هذه العينة من المجرمين وكذا هدف أو دافع كلّ هذه الفئة من ارتكاب الجريمة ومن جهـة أخرى تطرقنا إلى السمات المميزة لجرائم المعلوماتية عن غيرها من الجـرائم الأخـرى، ومجال ارتكابها، وفي الأخير وسائل الحماية من الجريمـة المعلوماتيـة، وكـذا الأوامـر الأساسية لأمن الأنترنت.

تطرقنا في بحثنا هذا المتواضع إلى جريمة الساعة، على الساحة القانونية الدولية بصفة
مة، فالعالم يجد صعوبات في التغلب على هذه الجريمة والقضاء عليها بسبب اتساع
اق الشبكة و الطابع الدولي لها، و الطفرات التكنولوجية المعقدّة في هذا المجال، أي
نترنت فقد حاولنا قدر المستطاع الالمام بالموضوع من خلال من خلال تعرضنا إلى
مية هذه الجريمة في الفصل الأوّل وميكانيزمات ودوافع ارتكابها في الفصل الثاني.
. توصلنا إلى أن الجريمة المعلوماتية مرتبطة بالتطور التكنولوجي الذي يشهده العالم
مفة عامة و بالتطور المذهل للحاسب الآلي ونظمه وسبل الاتصال وكذا اتساع رقعة

المـلاحظات:

1. عدم وجود تنسيق دولي وسلطة مركزية تهيمن على نشاط الشبكة و التحكم فيها.
2. عدم وجود جهات مختصة للبحث و الدراسة و التخطيط و التشريع في مجال الجريمة المعلوماتية على المستوى الدولي.
3. عدم وجود تنظيم للنصوص القانونية التي لا تزال طور الإحاطة و التغطية.

الاقتراحات:

1. نرجو من المشرع استصدار القانون المتعلق بهذه الجرائم المتحدثة (التصديق على مشروع القانون الذي يعدل ويتمم الأمر رقم 66-156 المؤرخ في هـ الموافق لـ 8 جوان سنة 1966 و المتضمن قانون العقوبات).وإردافه بنصوص أخرى تكفل بحماية تقنية المعلوماتية من شتى صور الاعتداء عليها.
2. نأمل من استحداث تخصصات تعنى بالبحث و الدراسة في موضوع الجرائم المعلوماتية ولِما لا انشاء معهد وطني لدراسة الجرائم المعلوماتية و الجرائم المستحدثة.
3. تشجيع الباحثين إلى التطرق إلى هذا الموضوع لأنّه حقل خصب لم يستغلّ بعد وذلك من خلال توجيه الأساتذة الطلبة للبحث و انجاز المذكرات في هذا الموضوع، ممّا يسمح باثراء الساحة القانونية الجزائرية بآراء وتحليلات مسائل قد يغفلها المشرع نظرا لحداثة الموضوع.

في النهاية، فإنّنا نتوجه إلى زملائنا الطلبة ونشجعهم على الخوض والبحث في هذا الموضوع، خاصة كونه موضوع الساعة، مطروح على الساحة الدولية، خاصة أن القضاء الجزائري يفتقر لاجتهادات قضائية فيما يخص هذه الجريمة. فإنّنا نأمل بعد استصدار القانون المطروح حاليا سلاحا في يد القاضي الجزائري للحكم في قضية تخص الجريمة المعلوماتية، إضافة إلى هذا القانون و الأحكام التي ستكون لاحقا والبحوث خاصة من الجانب التطبيقي وكذا بالتطور التكنولوجي والتحرر الاقتصادي، كلّها عوامل تؤدي حتما إلى انتشار مثل هذه الجريمة، لأن هذه الأخيرة وإن كانت مرتبطة بعدّة جوانب إلا أنّ الطابع الاقتصادي يغلب عليها.

"والله وليّ التوفيق"

المراجع

المراجع :

1- الدكتورة هدى قشوش : "جرائم الحاسب الإلكتروني في التشريع المقارن"، الطبعة الأولى، دار النهضة العربية، القاهرة، 1992.
2- الأستاذ الدكتور كامل السعيد : "شرح الأحكام العامة في قانون العقوبات الأردني و القانون المقارن"، الطبعة الثانية، دار الفكر للنشر و التوزيع، عمان، 1983.
3- الأستاذ الدكتور محمود نجيب حسني : "شرح قانون العقوبات- القسم العام"، الطبعة السادسة، دار النهضة العربية، القاهرة، 1989.
4- الدكتور سامي الشوا : " الغش المعلوماتي كظاهرة إجرامية مستحدثة"، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 1993.
5- الدكتور هشام فريد رستم : " قانون العقوبات و مخاطر تقنية المعلومات"، مكتبة الآلات الحديثة، أسيوط، 1992.
6- الأستاذ الدكتور أحمد فتحي سرور : " الوسيط في قانون العقوبات- القسم العام"، الطبعة الخامسة، دار النهضة العربية، القاهرة، 1991.
7- الدكتورة فوزية عبد الستار: " شرح قانون العقوبات- القسم العام"، دار النهضة العربية، القاهرة، 1992.
8- الأستاذ محي الدين عوض: " مشكلات السياسة الجنائية المعاصرة في جرائم المعلومات" ورقة عمل مقدمة إلى المؤتمر السياسي السادس للجمعية المصرية للقانون الجنائي، القاهرة، 1993.
9- الأستاذ (Ubrich Seiber) : " جرائم الحاسب الآلي و الجرائم الأخرى المرتبطة بالتقنيات الحديثة لوسائل الاتصال"، ترجمة الدكتور سامي الشوا، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، 1993، و الورقة ذاتها من أوراق التحضير للمؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات، البرازيل، 1994.
10- الدكتور محمد العريان : " الجرائم المعلوماتية"، دار الجامعة الجديدة للنشر، الإسكندرية، 2004.
11- Pieere catala, "Ebauche Dune Théorie Juridique de l'information" Andre, 1983.
12- الموقع : www.goa.gov
13- الموقع : www.oecd.org
14- الموقع : www.gocsi.com

الملحقات

متى تتحول الوقائع والاحداث الغريبة الى ظاهرة في خصوص ما ؟؟

انها تمسي ظاهرة حقيقية متى ما ازدادت الأحداث ضمن نسق معين ، ومتى ما تشكلت سمات للحدث الحاصلِ في نطاقها ، وللأثر المترتب على الحدث .

وهكذا ، ثمة ظاهرة حقيقية بشان جرائم المعلوماتية والانترنت ، فما هي ملامحها ، وما هو حجمها ، وماذا عن نطاق الخسائر الناجم عنها ؟؟

لدى الحديث عن واقع ونطاق ظاهرة جرائم الكمبيوتر والإنترنت يتعين ابتداء ان ندرك انه ليس ثمة دراسات إحصائية شاملة وليس ثمة اكثر من تقديرات تتباين دقتها تبعا لقدرة الجهات القائمة على إنجاز مثل هذه الدراسات ومدى موضوعيتها ، وفي هذا النطاق فان هناك فرقا حقيقيا بين دراسات الجهات غير الربحية وبين المؤسسات التجارية التي غالبا ما تكون دراساتها موجهة لغرض ما فتجيء النتائج معبرة عن هذا التوجه . ومن هذه الزاوية فان ما يعتمده هذا الدليل كامثلة على الدراسات المسحية يركز بشكل رئيس على دراسات الجهات الحكومية او غير الربحية ما امكن .

ومن المهم أيضا ادراك حقيقة ثانية ، ان الارقام المتوفرة من الدراسات الموضوعية ، لا تعكس باي صورة واقع الظاهرة بل تقدم صورة عن حقائقها العامة ، وفي حالة جرائم الكمبيوتر والإنترنت ، فان حجم الظاهرة ونطاق الجريمة وحجم المخاسر سيكون بالضرورة اكثر مما تقدمه هذه الدراسات من

نتائج ، مصدر ذلك حقيقة أخرى باتت معلومة للكافة وتستند الى اساس موضوعي وحقيقة منطقية ، وهي ان غالبية المؤسسات تسعى الى كتم خسائرها بل ربما تعمد الى اخفاء كل حقيقة تتصل بتعرضها لاية جريمة من جرائم الكمبيوتر والإنترنت حماية لثقة زبائنها بها وتمسكا امام الآخرين بفعالية نظام الأمن لديها . وهذا ما يعبر عنه في الدراسات البحثية بالرقم الاسود.

اعلن معهد أمن المعلومات **Computer Security Institute** نتائج تقرير عام 2001 وهو التقرير السادس حول جرائم الكمبيوتر ودراسة أمن المعلومات المسحية **2001 CSI/FBI Computer Crime and Security Survey** ، وهذه الدراسة يتم إجراؤها سنويا من قبل المعهد بتعاون مع مكتب التحقيقات الفدرالية في الولايات المتحدة الأمريكية ، بغرض رفع مستوى الوعي لمسائل أمن المعلومات وتحديد واقعها .

وقد اجريت هذه الدراسة الشاملة بمشاركة 538 مؤسسة أمريكية تضم وكالات حكومية و بنوك ومؤسسات مالية ومؤسسات صحية وجامعات ، واظهرت بوجه عام تنامي خطر جرائم الكمبيوتر وارتفاع حجم الخسائر الناجمة عنها بالرغم من زيادة الوعي بإلحاق المعلومات ، فقد تبين ان 85% من المشاركين في الدراسة وتحديدا المؤسسات الحكومية الكبرى تحرت اختراقات كمبيوتر خلال السنة

السابقة ، وان 64% لحقت بهم خسائر مادية جراء هذه الاعتداءات وان 35% تمكن من حساب مقدار خسائره المادية التي بلغت تقريبا 378 مليون دولار في حين كانت الخسائر لعام 2000 بحدود 265 مليون دولار وان معدل الخسارة السنوية لاعوام الثلاثة السابقة لعام 2000 بلغت 120 مليون دولار ، وان اخطر مصادر الخسارة المالية تمثل بسرقة المعلومات المتعلقة بالاموال والممتلكات (حوالي 151 مليون) والاحتيال المالي (حوالي 93 مليون) . واظهرت الدراسة أيضا ان 70% من الاعتداءات حصلت من نقطة الاتصال الخارجي عبر الإنترنت مقابل 30% حصلت من نقطة تتعلق بداخل النظام نفسه ، في حين كانت نسبة الاختراق عبر اتصال الإنترنت 59% في عام 2000 .

ان 36% من المشاركين بالدراسة قد ابلغوا جهات القانون حول هذه الاختراقات بزيادة بنسبة 11% عن عام 2000 ، حيث كانت نسبة المبلغين 25% عام 2000 في حين كانت 16% عام 1996 .

اما حول مصدر وطبيعة الاعتداءات فان 40% من الاعتداءات تمت من خارج المؤسسات مقابل 25% في عام 2000 ، وان 38% من الاعتداءات تعلقت **بهجمات انكار الخدمة** مقابل 27% عام 2000 وان نسبة الموظفين الذين ارتكبوا أفعال إساءة استخدام اشتراك الإنترنت لمنافع شخصية بلغت 91% ، تتوزع بين الاستخدام الخاطئ للبريد الإلكتروني وتنزيل مواد اباحية من الشبكة ، في حين

كانت هذه النسبة 79% في عام 2000 ، وان 94% من المشاركين تعرضوا لهجمات الفيروسات مقابل 85% عام 2000 .

وفيما يتعلق بالتجارة الإلكترونية ، فان 97% من المشاركين لديهم مواقع على الإنترنت ، وان 47% منهم يتعامل بالتجارة الإلكترونية ، وان 23% قد تعرضوا لدخول غير المصرح به او إساءة الاستخدام وان 27% لا يعرفون فيما اذا كانت مواقعهم قد تعرضت لمثل هذه الاعتداءات ، وان 21% من الجهات المشاركة التي تعرضت الاعتداءات أبلغت عن 2-5 حوادث وان 58% ابلغ عن عشرة حوادث فاكثر ، وان 90% من الاعتداءات كانت اعتداءا حاقدة مقابل 64% عام 2000 ، وان 78% من الاعتداءات تتعلق بانكار الخدمة مقابل 60% عام 2000 وان 13% ابلغوا عن سرقة معلومات مقابل 8% عام 2000 وان 8% ابلغوا عن احتيال مالي مقابل 3% عام 2000 .

ووفقا لتقرير حديث لمكتب المحاسبة في الولايات المتحدة الأمريكية فان عدد الحوادث التي تعامل معها فريق سيرت CERT (وهو فريق فدرالي للتدخل السريع بشان الجريمة الإلكترونية) ازداد من 1343 حادثا عام 1993 الى 9859 حادثا في عام 1999 .

والاحداث الشهيرة في هذا الحقل كثيرة ومتعددة لكننا نكتفي في هذا المقام بايراد ابرز الحوادث التي حصلت خلال السنوات الماضية بحيث نعرض لحوادث قديمة نسبيا وحديثة كامثلة على تنامي خطر هذه الجرائم وتحديدا في بيئة الإنترنت ، كما سنورد امثلة من خلاصات تقارير المحاكم حول بعضالوقائع الشهيرة مع الاشارة الى مواقع نشرها على شبكة الانترنت .

- **قضية مورس:-** هذه الحادثة هي أحد اول الهجمات الكبيرة والخطرة في بيئة الشبكات ، ففي تشرين الثاني عام 1988 تمكن طالب يبلغ من العمل 23 عاما ويدعى ROBER MORRIS من اطلاق فايروس عرف باسم (دودة مورس) عبر الإنترنت ، أدى الى اصابة 6 آلاف جهاز يرتبط معها حوالي 60000 نظام عبر الإنترنت من ضمنها اجهزة العديد من المؤسسات والدوائر الحكومية ، وقد قدرت الخسائر لاعادة تصليح الأنظمة وتشغيل المواقع المصابة بحوالي مائة مليون دولار اضافة الى مبالغ اكثر من ذلك تمثل الخسائر غير المباشرة الناجمة عن تعطل هذه الأنظمة ، وقد حكم على مورس بالسجن لمدة 3 اعوام وعشرة آلاف غرامة.

- **قضية الجحيم العالمي** :- تعامل مكتب التحقيقات الفدرالية مع قضية اطلق عليها اسم مجموعة الجحيم العالمي **GLOBAL HELL** فقد تمكنت هذه المجموعة من اختراق مواقع البيت الابيض والشركة الفدرالية الأمريكية والجيش الامريكي ووزارة الداخلية الأمريكية ، وقد

أدين اثنين من هذه المجموعة جراء تحقيقات الجهات الداخلية في الولايات المتحدة ، وقد ظهر من التحقيقات ان هذه المجموعات تهدف الى مجرد الاختراق اكثر من التدمير او التقاط المعلومات الحساسة ، وقد امضى المحققون مئات الساعات في ملاحقة ومتابعة هذه المجموعة عبر الشبكة وتتبع آثار أنشطتها ، وقد كلف التحقيق مبالغ طائلة لما تطلبه من وسائل معقدة في المتابعة .

- **فايروس ميلسا** :- وفي حادثة هامة أخرى ، انخرطت جهات تطبيق القانون وتنفيذه في العديد من الدول في تحقيق واسع حول اطلاق فايروس شرير عبر الإنترنت عرف باسم فايروس MELISSA حيث تم التمكن من اعتقال مبرمج كمبيوتر من ولاية نيوجرسي في شهر نيسان عام 1999 واتهم باختراق اتصالات عامة والتآمر لسرقة خدمات الكمبيوتر ، وتصل العقوبات في الاتهامات الموجهة له الى السجن لمدة 40 عام والغرامة التي تقدر بحوالي 500 الف دولار وقد صدر في هذه القضية مذكرات اعتقال وتفتيش بلغ عددها 19 مذكرة .

- **حادثة المواقع الاستراتيجية** :- وفي 19 تشرين الثاني 1999 تم ادانة **Eric burns** من قبل محكمة فيرجينيا الغربية بالحبس لمدة 15 شهرا والبقاء تحت المراقبة السلوكية لمدة 3 سنوات بعد ان اقر بذنبه وانه قام وبشكل متعمد باختراق كمبيوترات محمية الحق فيها ضررا بالغا في كل من ولايات فيرجينيا واشنطن واضافة الى لندن في بريطانيا ، وقد تضمن هجومه الاعتداء على مواقع لحلف الاطلسي اضافة الى الاعتداء على موقع نائب رئيس الولايات المتحدة كما اعترف بانه قد اطلع غيره من الهاكرز على الوسائل التي تساعدهم في اختراق كمبيوترات البيت الابيض ، وقد قام eric بتصميم برنامج اطلق عليه web bandit ليقوم بعملية تحديد الكمبيوترات

المرتبطة بشبكة الإنترنت التي تتوفر فيها نقاط ضعف تساعد على اختراقها ، وباستخدام هذا البرنامج اكتشف ان الخادم الموجود في فيرجينيا والذي يستضيف مواقع حكومية واستراتيجية منها موقع نائب الرئيس يتوفر فيه نقاط ضعف تمكن من الاختراق ، فقام في الفترة ما بين آب 1998 وحتى كانون الثاني 1999 باختراق هذا النظام 4 مرات ، واثر نشاطه على العديد من المواقع الحكومية التي تعتمد على نظام وموقع USIA للمعلومات ، وفي إحدى المرات تمكن من جعل آلاف الصفحات من المعلومات غير متوفرة مما أدى الى اغلاق هذا الموقع لثمانية ايام ، كما قام بالهجوم على مواقع لثمانين مؤسسة أعمال يستضيفها خادم شبكة LASER.NET في منطقة فيرجينيا والعديد من مؤسسات الاعمال في واشنطن اضافة الى جامعة واشنطن والمجلس الاعلى للتعليم في فيرجينيا رتشموند ومزود خدمات إنترنت في لندن ، وكان عادة يستبدل صفحات المواقع بصفحات خاصة به تحت اسم ZYKLON او باسم الامرأة التي يحبها تحت اسم CRYSTAL .

- **الاصدقاء الاعداء** :- وفي حادثة أخرى تمكن أحد الهاكرز (الإسرائيليين) من اختراق أنظمة معلومات حساسة في كل من الولايات المتحدة الأمريكية والكيان الصهيوني ، فقد تمكن أحد المبرمجين الإسرائيليين في مطلع عام 1998 من اختراق عشرات النظم لمؤسسات عسكرية ومدنية وتجارية في الولايات المتحدة وإسرائيل ، وتم متابعة نشاطه من قبل عدد من المحققين في الولايات المتحدة الأمريكية حيث اظهرت التحقيقات ان مصدر الاختراقات هي كمبيوتر موجود في الكيان الصهيوني فانتقل المحققون الى الكيان الصهيوني وتعاونت معهم جهات تحقيق إسرائيلية

حيث تم التوصل للفاعل وضبطت كافة الاجهزة المستخدمة في عملية الاختراق ، وبالرغم من ان المحققين أكدوا ان المخترق لم يتوصل الى معلومات حساسة الا ان وسائل الاعلام الأمريكية حملت أيضا أخبارا عن ان هذا الشخص كان في الاساس يقوم بهذه الانشطة بوصفه عميلا (لإسرائيل) ضد الولايات المتحدة الأمريكية.

- **حادثة شركة اوميغا** :- مصمم ومبرمج شبكات كمبيوتر ورئيس سابق لشركة omega من مدينة Delaware ويدعى Timothy Allen Lioyd (35 عاما) تم اعتقاله في 1998/2/17 بسبب إطلاقه قنبلة إلكترونية في عام 1996 bomb بعد 20 يوما من فصله من العمل استطاعت ان تلغي كافة التصاميم وبرامج الانتاج لاحد كبرى مصانع التقنية العالية في نيوجرسي والمرتبطة والمؤثرة على نظم تحكم مستخدمة في nasa والبحرية الأمريكية ، ملحقا خسائر بلغت 10 مليون دولار وتعتبر هذه الحادثة مثالا حيا على مخاطر جرائم التخريب في بيئة الكمبيوتر بل اعتبرت انها اكثر جرائم تخريب الكمبيوتر خطورة منذ هذه الظاهرة .

وحيث أننا سنقف – في أكثر من مقام في هذه الدراسة – على المعالم الرئيسة لخطورة هذه الجرائم ولحجم الخسائر الناجمة عنها عند تعرضنا لأنماطها وفئاتها والتمثيل على ذلك من واقع ملفات القضاء المقارن ، فاننا نكتفي في هذا المقام بايراد أبرز مخاطرها عموما، اضافة لما ذكرناه في البند الخاص بانواع الاعتداءات والهجمات :-

1- تهدد جرائم الحاسوب عموما الحق في المعلومات – انسيابها وتدفقها واستخدامها، وهذا الحق، وان يكن لما يزل محل نقاش مستفيض في اطار حقوق الجيل الثالث المؤسسة على

التضامن، فان الأهمية الاستراتيجية والثقافية والاقتصادية للمعلومات، تجعل من أنماط الاعتداء عليها خطورة جد بالغة بكونها تهدد في الحقيقة البناء الثقافي والاقتصادي للدولة، وأثر ذلك الواسع على التنمية التي اعترف بها كحق مِقرر للمجتمعات تجب حمايته ورعايته لكسر الهوة بين المجتمعات الفقيرة والغنية.

2- ان بعض جرائم الحاسوب تمس الحياة الخاصة أو ما يسمى بحق الانسان في الخصوصية، وهذه الجرائم تخلف وراءها – الى جانب الضرر الكبير بالشخص المستهدف في الاعتداء – شعورا عريضا لدى الافراد بمخاطر التقنية ، من شانه ان يؤثر سلبا في تفاعل الانسان مع التقنية ، هذا التفاعل اللازم لمواجهة تحديات العصر الرقمي .

3- تطال بعض جرائم الكمبيوتر الأمن القومي والسيادة الوطنية في اطار ما يعرف بحروب المعلومات او الأخلاقية الإلكتروني – الذي سبق عرض مفهومهما – وتحديدا جرائم التجسس وجرائم الاستيلاء على المعلومات المنقولة خارج الحدود .

4- تشيع جرائم الكمبيوتر والإنترنت فقدان الثقة بالتقنية ، لا فحسب لدى الأفراد – كما أسلفنا آنفا – وانما لدى اصحاب القرار في الدولة ، وهو ما سيؤثر في الحقيقة على استخدام التقنية في غير قطاع من قطاعات المجتمع ، وبدوره يؤثر على امتلاك الدولة للتقنية التي أصبحت تمثل حجر الزاوية في جهود التنمية وتطور المجتمع. ان جرائم الكمبيوتر وليدة التقنية تهدد التقنية ذاتها ، وبالتالي تهدد الفجر المشرق للمستقبل ، المؤسس على التفاعل الإيجابي ما بين الانسان والتقنية العالية.

ان خطر جرائم الكمبيوتر والإنترنت - أو بعضها على نحو أدق - لا يمس التقنية ذاتها في درجة شيوع الثقة بها سواء لدى الأفراد أو الدولة فحسب ، بل تهدد - أي الجرائم - مستقبل صناعة التقنية وتطورها ، وهذا يتحقق في الواقع من ثلاث فئات من جرائم الكمبيوتر والإنترنت ، جرائم قرصنة البرمجيات (Piracy) وجرائم التجسس الصناعي ، وجرائم احتيال الإنترنت المالي .

لجداول و الاعمدة البيانية

جدول 1 : خسائر جرائم الكمبيوتر وفق الدراسة المتقدمة للاعوام من 97 وحتى الربع الاول من 2001

مصدر الخسائر / الجريمة ونوع الهجوم	1997	1998	1999	2000	2001
Theft of proprietary info. سرقة المعلومات المتعلقة بالملكية	20,.48,000	33,545,000	42,496,000	66,708,000	151,230,100
Sabotage of data networks إتلاف او تخريب معطيات الشبكات	4,285,850	2,142,000	4,421,000	27,148,000	5,183,100
Telecom eavesdropping تصنت الشبكات	1,181,000	562,000	765,000	991,200	886,000
System Penetration by outsider اختراق النظام من الخارج	2,911,700	1,637,000	2,885,000	7,885,000	19,066,600
Insider abuse of Net access إساءة الدخول للشبكة من داخل المنشأة	1,006,750	3,720,000	7,576,000	27,984,740	35,001,650
Financial Fraud الاحتيال المالى	24,892,000	11,239,000	39,706,000	55,996,000	92,935,500
Denial of Service انكار الخدمة	N/a	2,787,000	3,255,000	8,247,500	4,283,600
Spoofing التلاعب والخداع بطريق سبوفنغ	512,000	N/a	N/a	N/a	N/a
Virus الفايروسات	12,498,150	7,874,000	5,274,000	29,171,700	45,288,150
Unauthorized insider Access الدخول غير المصرح به من الداخل	3,991,605	50,565,000	3,567,000	22,554,500	6,064,000
Telecom Fraud احتيال الاتصال	22,660,300	17,256,000	773,000	4,028,000	9,041,000
Active Wiretapping استراق السمع – المادى -	N/a	245,000	20,000	5,000,000	0
Laptop Theft سرقة الكمبيوتر المحمول	6,132,200	5,250,000	13,038,000	10,404,300	8,849,000
المجموع	**100,119,55**	**136,822,00**	**123,799,00**	**265,586,24**	**377,828,700**

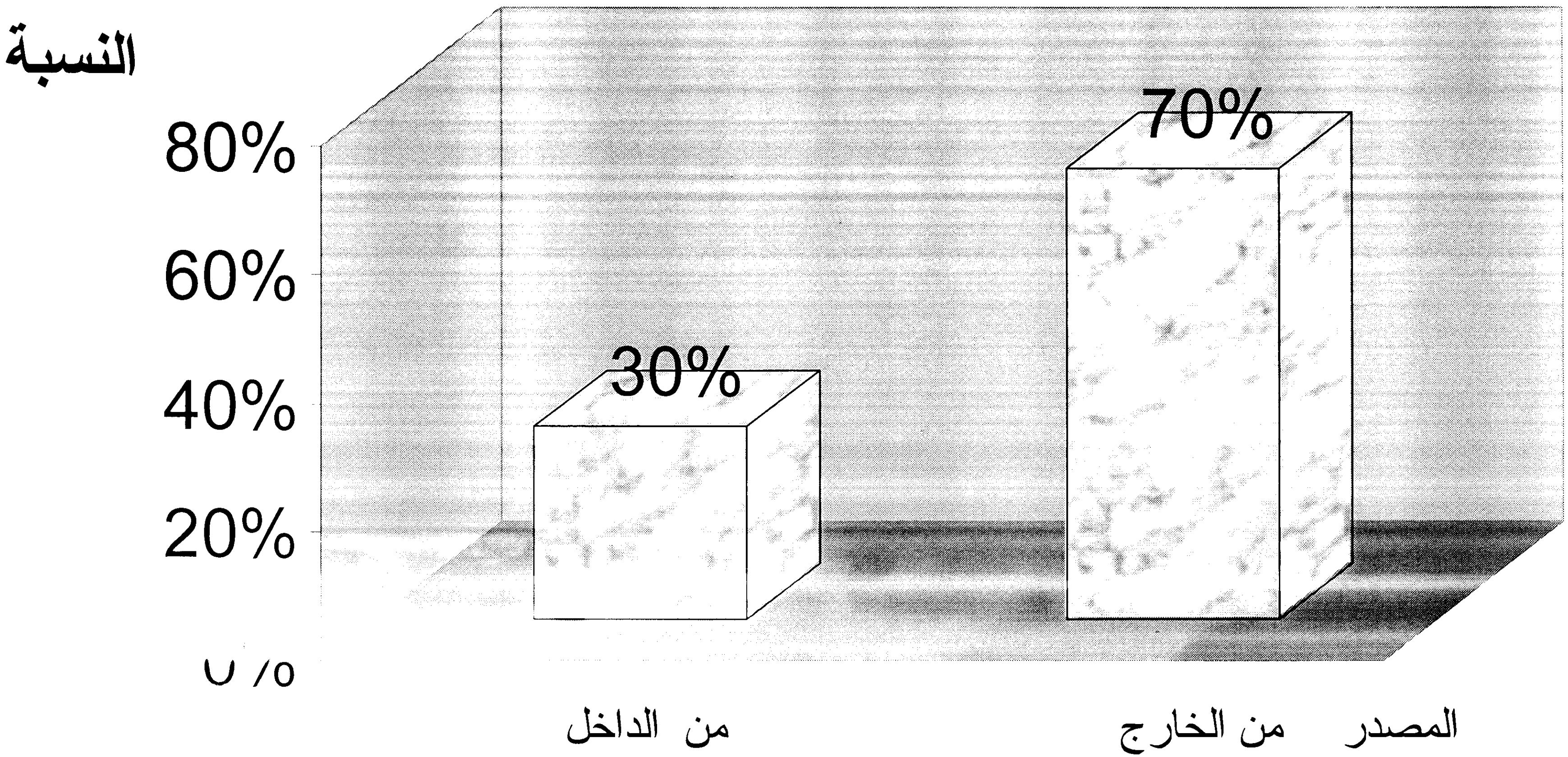
عن معهد أمن المعلومات **Computer Security Institute** نتائج تقرير عام 2001 وهو التقرير السادس حول جرائم الكمبيوتر ودراسة أمن المعلومات المسحية **2001 CSI/FBI Computer Crime and Security Survey** ، وهذه الدراسة يتم إجراؤها سنويا من قبل المعهد بتعاون مع مكتب التحقيقات الفدرالية في الولايات المتحدة الأمريكية

جدول 2: وسيلة اكتشاف الجريمة المعلوماتية

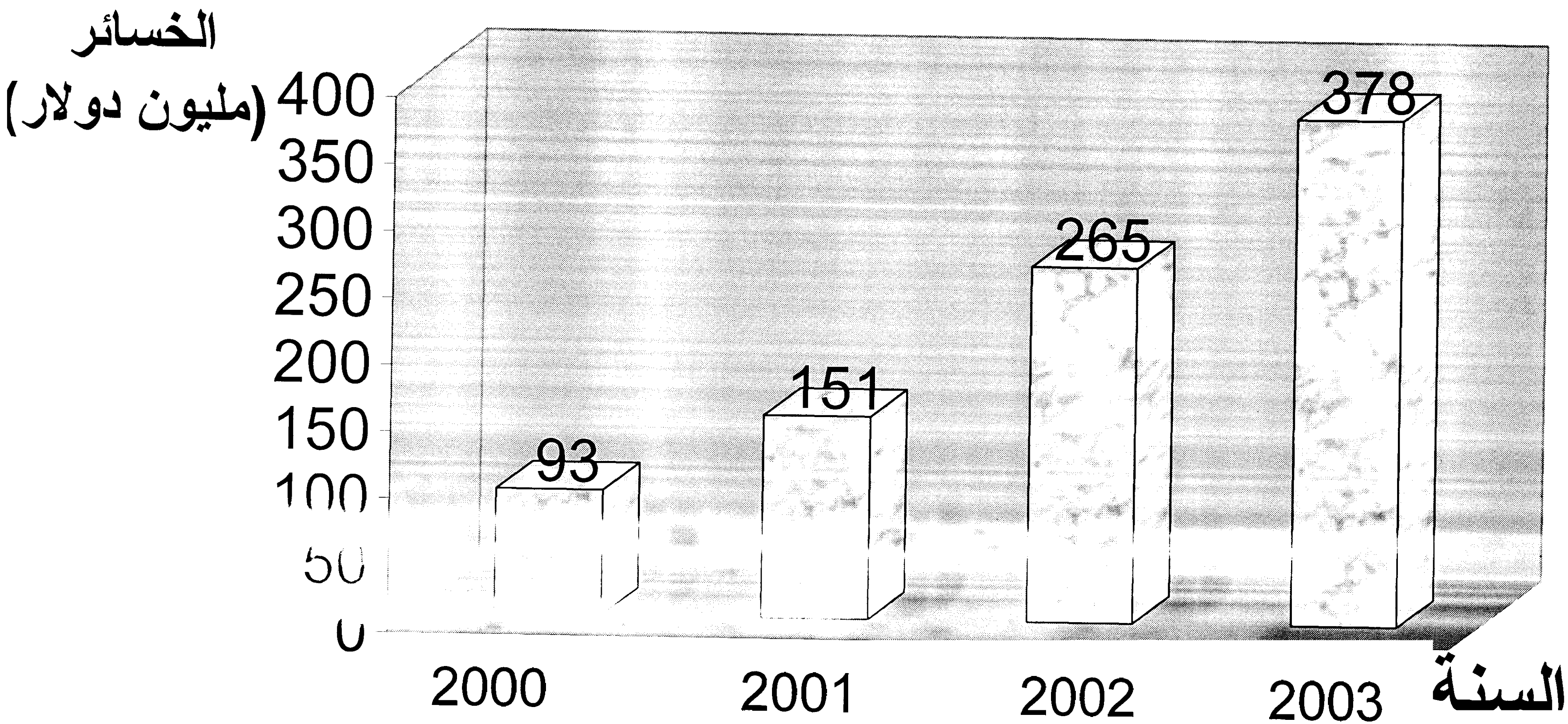
وسيلة اكتشاف الجريمة المعلوماتية	النسبة المئوية
يقظة و دقة الإدارة و مهارتها في الرقابة	**15%**
شكاوى قدمها المجني عليهم	**10%**
إثر إجراء تغييرات في الإدارة و برمجة التطبيقات الجديدة	**07%**
بمحض الصدفة	**15%**
معلومات سرية للشرطة و لرب العمل الذي يعمل لديه الفاعل	**15%**
شك و ريب من جانب الإدارة أو الزملاء	**3%**

التقرير السنوي الثاني الصادر عن مؤسسة (Erust et Young) مؤسسة متخصصة في خدمات الأعمال و الرقابة و الاستشارات، و تعد من المؤسسات في هدا الحقل برأسمال 9 بليون و بعدد موظفين يصل إلى 30 ألف في 130 دولة في العالم.

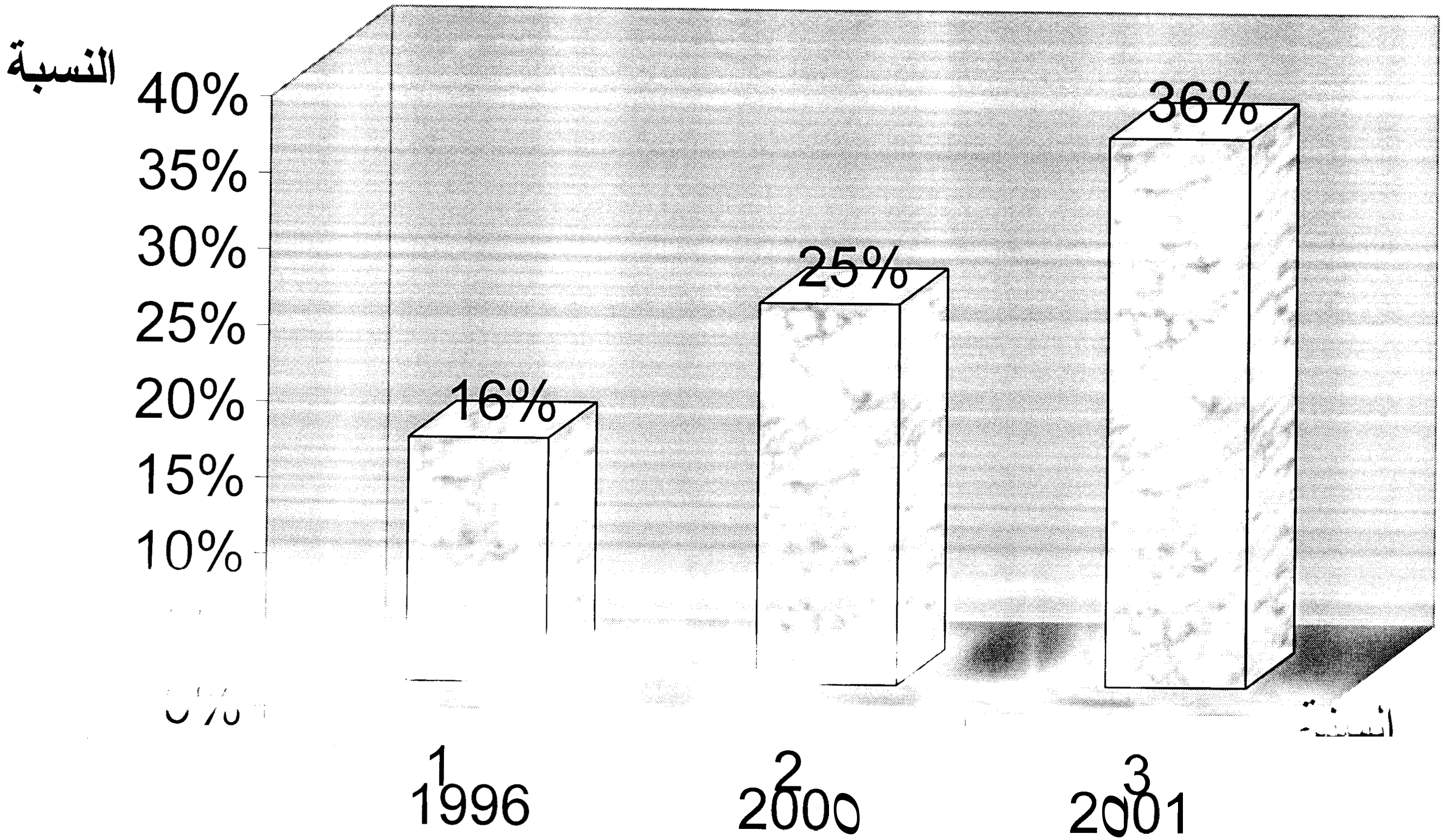
مصدر الجريمة المعلوماتية :



الخسائر الناجمة عن الجريمة المعلوماتية:



نسبة الأشخاص المبلغين عن الجريمة:



مشـــروع قانـــون يعدل ويتمم الأمر رقم 66-156
المـــؤرخ في 18 صفـــر عام 1386
الموافـــق لـــ 8 يونيـــو سنة 1966
والمتضمـــن قانـــون العقوبـــات

أكتوبر 2003

الجمهورية الجزائرية الديمقراطية الشعبية

مشروع قانون رقم... المؤرخ في ... الموافق...
المعدل و المتمم للأمر رقم 66-156 المؤرخ في 18 صفر 1386 الموافق
8 جوان 1966 المتضمن قانون العقوبات

(عرض الأسباب)

يندرج مشروع هذا القانون الذي يعدل ويتمم قانون العقوبات في إطار مواصلة إصلاح العدالة، تكملة للمخطط الاستعجالي الذي بادرت به وزارة العدل في سنة 2001 وتجسيدا لتوصيات اللجنة الوطنية لإصلاح العدالة المتعلقة بضرورة إعادة النظر في مجمل النصوص القانونية لهذا القطاع.

ويهدف هذا المشروع إلى تكييف قانون العقوبات مع التحولات السياسية والاقتصادية والاجتماعية التي تعرفها بلادنا، قصد التكفل بالأشكال الجديدة للإجرام الناتجة عنها، كون ظاهرة الإجرام مرتبطة ارتباطا وثيقا بحركية المجتمع، الأمر الذي يقتضي التحيين المستمر والدائم للقوانين الجزائية التي تشكل الأداة التي تمكن الدولة من الحفاظ على النظام العام داخل المجتمع وتضمن من خلالها حماية حقوق الأفراد وحرياتهم واستتباب الأمن والاستقرار والسلم، بتجريم الأفعال التي تهدد الأمن الفردي والجماعي وتقرير العقوبات الملائمة لها.

كما يهدف أيضا إلى مجانسة القانون الوطني مع المعايير الدولية والالتزامات الاتفاقية لبلادنا .

وفي هذا الإطار، يهدف هذا المشروع إلى التكفل ضمن قانون العقوبات بما يلي:

1- تكريس مبدأ المسؤولية الجزائية للشخص المعنوي في القسم العام من قانون العقوبات:

لقد نص المشرع الجزائري على المسؤولية الجزائية للشخص المعنوي في قانون العقوبات (المادة 144 مكرر 1 المتعلقة بمسؤولية النشرية عن جريمة الإهانة) كما نص عليها في بعض القوانين الخاصة التي من بينها القانون المتعلق بحماية البيئة والأمر المتعلق بحركة رؤوس الأموال من وإلى الخارج وكذا في المادة 646 وما بعدها من قانون الإجراءات الجزائية التي تنص على مسك صحيفة السوابق القضائية للشركات المدنية والتجارية.

لذلك و تماشيا مع هذا التطور، يقترح إدراج ضمن القسم العام لقانون العقوبات أحكاما تتضمن العقوبات المطبقة على الشخص المعنوي وشروط قيام مسؤوليته.

وتجدر الإشارة إلى أن هذا التطور، يقتضي تكييف مجمل مواد قانون العقوبات قصد تحديد الجرائم التي يمكن أن يسأل عنها الشخص المعنوي.

وفي هذا الإطار ينص مشروع هذا القانون على المسؤولية الجزائية للشخص المعنوي في الأحكام المتعلقة بجمعية الأشرار والأحكام المتعلقة بتجريم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات.

و تجدر الإشارة أيضا إلى أن الأحكام المتعلقة بالمسؤولية الجزائية للشخص المعنوي لا تطبق على الدولة و الجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام.

2 – تدعيم الإطار التشريعي لمكافحة الجريمة المنظمة:

في هذا الإطار يقترح تعديل المادة 176 من قانون العقوبات والمتعلقة بجمعية الأشرار ليشمل مضمونها أيضا الجماعة الإجرامية المنظمة.

كما تم النص على تعريف الاشتراك في الجريمة المنظمة طبقا لأحكام اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

علاوة على ذلك، يقترح المشروع إدراج مسؤولية الأشخاص المعنوية وفقا للشروط المحددة في المادة 51 مكرر منه، وذلك بغرض خلق تجانس بين التعديلات المقترحة.

3-**تجريم التعذيب بكل أشكاله**: إن الهدف من تجريم التعذيب هو تدعيم الإطار التشريعي الوطني لحماية حقوق الإنسان وتطبيقا لأحكام اتفاقية نيويورك المتعلقة بمناهضة التعذيب وغيره من ضروب المعاملة أو العقوبة القاسية أو اللاإنسانية أو المهينة التي صادقت عليها الجزائر.

إن قانون العقوبات ينص على التعذيب في البعض من أحكامه دون أن يعرفه تعريفا شاملا ومانعا، **لذلك وتداركا للنقص الذي يعرفه تشريعنا في هذا المجال، يقترح إدراج ضمن قانون العقوبات لأحكام تجرم التعذيب كجريمة قائمة بذاتها وتنص على تشديد العقوبة إذا تم ارتكاب التعذيب من قبل موظف** (المواد 263 مكرر، 263 مكرر 1 و263 مكرر2).

A

4- النص على تجريم أفعال التحرش الجنسي:

إن التحرش الجنسي ظاهرة موجودة في مجتمعنا وتؤثر سلبا على علاقات العمل وعلى المساواة بين العمال في أماكن العمل وعلى مردودية العمل، لذلك واستجابة لطلبات العديد من الجمعيات والنقابات يقترح النص على تجريم التحرش الجنسي في قانون العقوبات لإعطاء الضحية الوسيلة القانونية التي تمكنها من المطالبة بحقوقها و متابعة المسؤول عن هذه الممارسات.

5- تجريم تبييض الأموال:

يقترح هذا المشروع في المادة 389 مكرر وما بعدها تجريم تبييض لأموال، عن طريق وضع أحكام قانونية تمكن من مكافحة هذه الآفة التي صبحت تهدد بصورة واضحة اقتصاديات الدول وتعرقل الصفقات الدولية.

وأن الهدف من عملية تبييض الأموال هو إخفاء المصدر غير المشروع للأموال وإدراجها في اقتصاد الدول وكذا مساعدة الأشخاص المتورطين في لإفلات من الآثار القانونية لأفعالهم.

لذلك فإن القضاء على هذه الآفة، يقتضي التعاون على أوسع نطاق بين جميع الدول،لأن هذا النوع من الإجرام يرتكب من قبل شبكات الإجرام الدولية.

وتندرج هذه الاقتراحات أيضا في نطاق تنفيذ الجزائر لالتزاماتها الناتجة عن مصادقتها على اتفاقية الأمم المتحدة للجريمة المنظمة .

6- تجريم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات:

إن التقدم التكنولوجي وانتشار استعمال وسائل الاتصال الحديثة، أدى إلى بروز أشكال جديدة للإجرام، مما دفع بالكثير من الدول إلى النص على معاقبتها.

و أن الجزائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات.

لذلك، فإن هذا المشروع في المواد من 394 مكرر إلى 394 مكرر7 يحدد الجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات مع النص كذلك على الجرائم الماسة بالدفاع الوطني و المؤسسات العمومية وتشديد العقوبات المقررة في هذه الحالة .

●●●●●

ويقترح أيضا العقوبات المطبقة على الأشخاص المعنوية التي تمس بأنظمة المعالجة الآلية للمعطيات.

إن هذه التعديلات من شأنها سد الفراغ القانوني في بعض المجالات وسوف تمكن لا محالة من مواجهة بعض أشكال الإجرام الجديد.

تجدر الإشارة أن التعديلات المقترحة تضمنت النص على غرامات جزائية مشددة في جميع الجرائم لا تقل في حدها الأدنى عن 50.000 دج وتبلغ في حدها الأقصى مبلغ 8.000.000 دج في بعض الجرائم .

ذالكـــم هو محتـــوى مشروع هذا القانـــون.

الجمهورية الجزائرية الديمقراطية الشعبية

مشروع قانون رقم .... المؤرخ في .....
الموافق ... يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966
المتضمن قانون العقوبات

إن رئيس الجمهورية،

بناء على الدستور، لا سيما المواد 119 و120 و122-7 و 126 منه ،

- وبمقتضى الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، المعدل والمتمم،

- وبمقتضى الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات ، المعدل والمتمم.

- وبعد مصادقة البرلمان .

يصدر القانون الآتي نصه :

المادة الأولى: يهدف هذا القانون إلى تعديل وتتميم الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون العقوبات.

المادة 2: يعدل ويتمم عنوان الباب الأول من الكتاب الأول من الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 والمذكور أعلاه، ويحرر كما يأتي:

الباب الأول

العقوبات المطبقة
على الأشخاص الطبيعية

المادة 3 : تتمم الفقرة 1 من المادة 5 من الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 والمذكور أعلاه، وتحرر كما يأتي:

" المادة 5: العقوبات الأصلية في مواد الجنايات:

1) ....،
2) ....،
3)......... .

ن عقوبات السجن لا تمنع تطبيق عقوبة الغرامة."

المــادة 4: يـتمم الكتاب الأول من الأمر رقــم 66-156 الـ خ ـي نيو سنة 1966 والمذكور أعلاه، بباب أول مكرر تحت عنوان " عقوبات مطبقــة على الأشخاص المعنوية " ، يشمل مادتين 18 مكرر و 18مكرر 1، ـ ـ ا كما يأتـ :

الباب الأول مكرر
العقوبات المطبقة على الأشخاص المعنوية

"المادة 18 مكرر: العقوبات التي تطبق على الشخص المعنوي في مواد ـنايات والجنح هي:

1-الغــرامة التــي تســاوي من مرة (1) إلى خمس(5) مرات الحد الأقصــى للغـرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

2-واحدة أو أكثر من العقوبات التالية:
- حل الشخص المعنوي،
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس (5) سنوات،
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس (5) سنوات،
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر، نهائيا أو لمدة لا تتجاوز خمس (5) سنوات،
-مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها،
- نشر وتعليق حكم الإدانة ،
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس (5) سنوات وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته."

"المادة 18 مكرر1: العقوبات التي تطبق على الشخص المعنوي في المخالفات هي:

الغرامة التي تساوي من مرة (1) إلى خمس(5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

كما يمكن الحكم بمصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها."

المادة 5 : يتمم الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 والمذكور أعلاه،بمادة 51 مكرر تحرر كما يأتي:

"المادة 51 مكرر : باستثناء الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام، يكون الشخص المعنوي، مسؤولا جزائيا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين عندما ينص القانون على ذلك.

إن مسؤولية الشخص المعنوي لا تمنع مساءلة الشخص الطبيعي كفاعل أصلي أو كشريك لنفس الأفعال."

2-واحدة أو اكثر من العقوبات التالية:
- حل الشخص المعنوي،
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس (5) سنوات،
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس (5) سنوات،
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر، نهائيا أو لمدة لا تتجاوز خمس (5) سنوات،
-مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها،
- نشر وتعليق حكم الإدانة ،
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس (5) سنوات وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته."

"المادة 18 مكرر1: العقوبات التي تطبق على الشخص المعنوي في المخالفات هي:

الغرامة التي تساوي من مرة (1) إلى خمس(5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

كما يمكن الحكم بمصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها."

المادة 5 : يتمم الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 والمذكور أعلاه،بمادة 51 مكرر تحرر كما يأتي:

"المادة 51 مكرر : باستثناء الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام، يكون الشخص المعنوي، مسؤولا جزائيا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين عندما ينص القانون على ذلك.

إن مسؤولية الشخص المعنوي لا تمنع مساءلة الشخص الطبيعي كفاعل أصلي أو كشريك لنفس الأفعال."

المـادة 6: تعدل وتتمم المادتان 176 و 177 من الأمر رقـم 66-156 المؤرخ في 8 يونيو سنة 1966 والمذكور أعلاه وتحرران كما يأتي:

"المـادة 176 : كـل جمعية أو اتفاق مهما كانت مدته و عدد أعضائه تشـكل أو تؤلف بغرض الإعداد لجناية أو أكثر، أو لجنحة أو أكثر معاقب علـيها بخمـس(5) سـنوات حبس على الأقل، ضد الأشخاص أو الأملاك تكـوّن جمعـية أشرار وتقوم هذه الجريمة بمجرد التصميم المشترك على العمل."

" المـادة 177: يعاقـب علـى الاشتراك في جمعية الأشرار بالسجن المؤقـت مـن خمـس (5) سـنوات إلى عشر (10) سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج، إذا تم الإعداد لارتكاب جنايات،

وتكون العقوبة الحبس من سنتين (2) إلى خمس (5) سنوات والغرامة من 100.000 د.ج إلى 500.000 دج، إذا تم الإعداد لارتكاب جنح.

ويعاقب منظم جمعية الأشرار أو من يباشر فيها أية قيادة كانت بالسجن المؤقت من عشر (10) سنوات إلى عشرين (20) سنـة وبغرامـة من 1.000.000 دج إلى 5.000.000 دج. "

المـادة 7: يـتمم الأمر رقـم 66-156 المؤرخ في 8 يونيو سنة 1966 والمذكور أعلاه بمادتين 177 مكرر و 177مكرر1، تحرران كما يأتي:

"المـادة 177 مكرر : دون الإخلال بأحكام المادة 42 من هذا القانون، يعد اشتراكا في جمعية الأشرار المنصوص عليها في هذا القسم :

1- كل اتفاق بين شخصين أو أكثر لأجل ارتكاب إحدى الجرائم المنصوص عليها في المادة 176 من هذا القانون وذلك بغرض الحصول على منفعة مالية أو مادية أخرى.

2-القيام عن علم بهدف جمعية الأشرار أو بعزمها على ارتكاب جرائم

[illegible]

أ- نشاط جمعية الأشرار وفي أنشطة أخرى تضطلع بها الجماعة مع علمه بان مشاركته ستساهم في تحقيق الهدف الإجرامي للجماعة.

ب- تنظيم ارتكاب جريمة من قبل جمعية الأشرار أو الإيعاز بارتكاب تلك الجريمة أو المساعدة أو التحريض عليه أو تيسيره أو إبداء المشورة بشأنه".

المادة 177 مكرر 1 : يكون الشخص المعنوي مسؤولا جنائيا وفقا للشروط المنصوص عليها في المادة 51 مكرر أعلاه، عن الجرائم المنصوص عليها في المادة 176 من هذا القانون ويعاقب بالغرامة التي تساوي خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي المنصوص عليها في المادة 177 من هذا القانون.

يطبق عليه أيضا واحدة أو أكثر من العقوبات التالية:

1- الإقصاء من الصفقات العمومية لمدة خمس (5) سنوات،

2- المنع لمدة خمس (5) سنوات من مزاولة بطريقة مباشرة أو غير مباشرة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته،

3 - مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.

المادة 8: يعدل ويتمم العنوان رقم 1 من القسم الأول من الفصل الأول من الباب الثاني من الكتاب الثالث من الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 والمذكور أعلاه، ويحرر كما يأتي:

I--القتل العمد والقتل مع سبق الإصرار و الترصد
وقتل الأصول والأطفال والتسميم والتعذيب

المادة 9 : يتمم الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 والمذكور أعلاه، بالمواد 263 مكرر و263 مكرر 1 و263 مكرر 2، وتحرر كما يأتي:

"المادة 263 مكرر: يقصد بالتعذيب كل عمل ينتج عنه ألما أو عذابا شديدا جسديا كان أو عقليا يلحق عمدا بشخص ما، مهما كان سببه".

"المادة 263 مكرر 1: يعاقب بالسجن المؤقت من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 100.000 دج إلى 500.000 دج كل من يمارس أو يحرض أو يأمر بممارسة التعذيب على شخص.

يعاقب على التعذيب بالسجن المؤقت من عشر (10) سنوات إلى عشرين (20) سنة وبغرامة من 150.000 دج إلى 800.000 دج، إذا سبق أو صاحب أو تلى جناية غير القتل العمد".

"المادة 263 مكرر 2: يعاقب بالسجن المؤقت من عشر (10) سنوات إلى عشرين (20) سنة وبغرامة من 150.000 دج إلى 800.000 دج، كل موظف يمارس أو يحرض أو يأمر بممارسة التعذيب من أجل الحصول على اعترافات أو معلومات أو لأي سبب آخر.

وتكون العقوبة السجن المؤبد، إذا سبق التعذيب أو صاحب أو تلى جناية غير القتل العمد.

يعاقب بالسجن المؤقت من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 100.000 دج إلى 500.000 دج، كل موظف يوافق أو يسكت عن الأفعال المذكورة في المادة 263 مكرر من هذا القانون".

المادة 10 : يتمم الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 والمذكور أعلاه، بمادة 341 مكرر تحرر كما يأتي :

"المادة 341 مكرر: يعد مرتكبا لجريمة التحرش الجنسي ويعاقب بالحبس من شهرين (2) إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج ، كل شخص يستغل سلطة وظيفته أو مهنته عن طريق إصدار الأوامر للغير أو بالتهديد أو الإكراه أو بممارسة ضغوط عليه قصد إجباره على الاستجابة لرغباته الجنسية".

المادة 11: يتمم الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 والمذكور أعلاه، بقسم سادس مكرر تحت عنوان: " تبييض الأموال" ويشمل المواد من 389 مكرر إلى 389 مكرر 7 تحرر كما يأتي:

القسم السادس مكرر

تبييض الأموال

المادة 389 مكرر : يعتبر تبييضا للأموال:

أ-تحويل الممتلكات أو نقلها مع علم الفاعل بأنها عائدات إجرامية، بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تأتت منها هذه الممتلكات، على الإفلات من الآثار القانونية لفعلته.

ب- إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو الحقوق المتعلقة بها، مع العلم بأنها عائدات إجرامية.

ج- اكتساب الممتلكات أو حيازتها أو استخدامها مع علم الشخص القائم بذلك وقت تلقيها، بأنها تشكل عائدات إجرامية.

د- المشاركة في ارتكاب أي من الجرائم المقررة وفقا لهذه المادة، أو التواطؤ أو التآمر على ارتكابها ومحاولة ارتكابها و المساعدة والتحريض على ذلك و تسهيله و إسداء المشورة بشأنه.

المادة 389 مكرر 1: يعاقب كل من قام بتبييض الأموال بالحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من1.000.000 د.ج إلى 3.000.000 د.ج."

"المادة 389 مكرر 2: يعاقب تبييض الأموال بالحبس من عشر (10) سنوات إلى خمسة عشرة (15) سنة و بغرامة من 4.000.000 دج إلى 8.000.000 دج، إذا ارتكب على سبيل الاعتياد أو باستعمال التسهيلات التي يمنحها نشاط مهني أو في إطار جماعة إجرامية."

"المادة 389 مكرر 3: يعاقب على المحاولة في الجرائم المنصوص عليها في هذا القسم بالعقوبات المقررة للجريمة التامة".

" المادة 389 مكرر 4: تحكم الجهة القضائية المختصة بمصادرة الأملاك موضوع الجريمة المنصوص عليها في هذا القسم، بما فيها العائدات والفوائد الأخرى الناتجة عن ذلك، في أي يد كانت، إلا إذا أثبت مالكها انه يحوزها بموجب سند شرعي وأنه لم يكن يعلم بمصدرها غير المشروع.

يمكن للجهة القضائية المختصة الحكم بمصادرة الأموال محل الجريمة عندما يبقى مرتكب أو مرتكبو التبييض مجهولين.

إذا اندمجت عائدات جناية أو جنحة مع الأموال المتحصل عليها بطريقة شرعية، فإن المصادرة لا يمكن أن تكون إلا بمقدار هذه العائدات.

كما تنطق الجهة القضائية المختصة بمصادرة الوسائل و المعدات المستعملة في ارتكاب جريمة التبييض.

إذا تعذر تقديم أو حجز الممتلكات محل المصادرة، تقضي الجهة القضائية المختصة بعقوبة مالية تساوي قيمة هذه الممتلكات.

يجب أن يتضمن الحكم أو القرار القاضي بالمصادرة تعيين الممتلكات المعنية و تعريفها وكذا تحديد مكانها".

"المادة 389 مكرر 5: يطبق على الشخص الطبيعي المحكوم عليه لارتكابه الجرائم المنصوص عليها في المادتين 389 مكرر 1 و 389 مكرر 2 واحدة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة 9 من هذا القانون.

"المادة 389 مكرر 6: يجوز الحكم بالمنع من الإقامة على الإقليم الوطني بصفة نهائية أو لمدة عشر (10) سنوات على الأكثر، على كل أجنبي مدان باحدى الجرائم المنصوص عليها في المادتين 389مكرر1 و 389 مكرر2 ".

"المادة 389 مكرر 7: يعاقب الشخص المعنوي الذي يرتكب الجريمة المنصوص عليها بالمادتين 389 مكرر1 و 389 مكرر2 بالعقوبات التالية:

- غرامة لا يمكن أن تقل عن أربع (4) مرات الحد الأقصى للغرامة المنصوص عليها في المادتين 389 مكرر1 و 389 مكرر2 من هذا القانون.

- مصادرة الممتلكات والعائدات التي تم تبييضها.

- مصادرة الوسائل والمعدات التي استعملت في ارتكاب الجريمة.

إذا تعذر تقديم أو حجز الممتلكات محل المصادرة تحكم الجهة القضائية المختصة بعقوبة مالية تساوي قيمة هذه الممتلكات.

ويمكن للجهة القضائية أن تقضي بالإضافة إلى ذلك بواحدة أو أكثر من العقوبات التالية:

أ- المنع من ممارسة نشاط مهني أو اجتماعي لمدة لا تتجاوز خمس (5) سنوات.

ب- حل الشخص المعنوي".

المادة 12 : يتمم الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 والمذكور أعلاه، بقسم سابع مكرر تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات "، يشمل المواد من 394 مكرر إلى 394 مكرر7 تحرر كما يأتي:

"القسم السابع مكرر
المساس بأنظمة المعالجة الآلية للمعطيات

" المادة 394 مكرر: يعاقب بالحبس من ثلاثة(3) أشهر إلى سنة(1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة(6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000 دج".

"المادة 394 مكرر1 : يعاقب بالحبس من ستة (6) أشهر إلى ثلاث(3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها."

"المادة 394 مكرر2 : يعاقب بالحبس من شهرين (2) إلى ثلاث(3) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج كل من يقوم عمدا وعن طريق الغش بـ:

1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصلة من إحدى الجرائم المنصوص عليها في هذا القسم".

"المادة 394 مكرر3: تضاعف العقوبات المنصوص عليها في هذا القسم. إذا استهدفت الجريمة الدفاع الوطني أو المؤسسات العمومية، دون الإخلال بتطبيق عقوبات أشد".

"المادة 394 مكرر4: يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس(5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي".

المادة 394 مكرر5 : كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها".

"المــادة 394 مكــرر6 : مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصــادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها".

"المــادة 394 مكــرر7: يعاقــب علـــى الشـــروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها. "

المادة 13: تلغى أحكام الفقرة 3 من المادة 110 مكرر من الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 والمذكور أعلاه.

المــادة 14 : ينشــر هذا القانون في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية.

حرر في :.........

الموافــق:.........

عبد العزيز بوتفليقة

المعاهدات و الاتفاقيات الدولية

معاهدة بودا بست

CouncilEurope

English

Convention sur la cybercriminalité

Budapest, 23.XI.2001

Rapport explicatif

Préambule

Les Etats membres du Conseil de l'Europe et les autres Etats signataires,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres;

Reconnaissant l'intérêt d'intensifier la coopération avec les autres Etats parties à la Convention;

Convaincus de la nécessité de mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyber-espace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale;

Conscients des profonds changements engendrés par la numérisation, la convergence et la mondialisation permanente des réseaux informatiques;

Préoccupés par le risque que les réseaux informatiques et l'information électronique soient utilisés également pour commettre des infractions pénales et que les preuves de ces infractions soient stockées et transmises par le biais de ces réseaux;

Reconnaissant la nécessité d'une coopération entre les États et l'industrie privée dans la lutte contre la cybercriminalité et le besoin de protéger les intérêts légitimes liés au développement des technologies de l'information ;

Estimant qu'une lutte bien menée contre la cybercriminalité requiert une coopération internationale en matière pénale accrue, rapide et efficace;

Convaincus que la présente Convention est nécessaire pour prévenir les actes portant atteinte à la confidentialité, l'intégrité et la disponibilité des systèmes informatiques, des réseaux et des données ainsi que l'usage frauduleux de tels systèmes, réseaux et données, en assurant l'incrimination de ces comportements, tels que décrits dans la présente Convention, et l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales, en en facilitant la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international, et en prévoyant des dispositions matérielles en vue d'une coopération internationale rapide et fiable ;

Gardant à l'esprit la nécessité de garantir un équilibre adéquat entre les intérêts de l'action

répressive et le respect des droits de l'homme fondamentaux, tels que garantis dans la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe (1950), dans le Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ainsi que dans d'autres conventions internationales applicables en matière de droits de l'homme, qui réaffirment le droit de ne pas être inquiété pour ses opinions, le droit à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées de toute nature, sans considération de frontière, ainsi que le droit au respect de la vie privée;

Conscients également de la protection des données personnelles, telle que la confère, par exemple, la Convention de 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Considérant la Convention des Nations Unies relative aux droits de l'enfant et la Convention de l'Organisation Internationale du Travail sur les pires formes de travail des enfants (1999) ;

Tenant compte des conventions existantes du Conseil de l'Europe sur la coopération en matière pénale, ainsi que d'autres traités similaires conclus entre les Etats membres du Conseil de l'Europe et d'autres Etats, et soulignant que la présente Convention a pour but de les compléter en vue de rendre plus efficaces les enquêtes et procédures pénales portant sur des infractions pénales en relation avec des systèmes et données informatiques, ainsi que de permettre la collecte des preuves électroniques d'une infraction pénale ;

Se félicitant des récentes initiatives destinées à améliorer la compréhension et la coopération internationales aux fins de la lutte contre la criminalité dans le cyber-espace, et notamment des actions menées par les Nations Unies, l'OCDE, l'Union européenne et le G8;

Rappelant la Recommandation N°(85) 10 concernant l'application pratique de la Convention européenne d'entraide judiciaire en matière pénale relative aux commissions rogatoires pour la surveillance des télécommunications, la Recommandation N° R (88) 2 sur des mesures visant à combattre la piraterie dans le domaine du droit d'auteur et des droits voisins, la Recommandation N° R(87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, la Recommandation N° R (95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques et la Recommandation n° R (89) 9 sur la criminalité en relation avec l'ordinateur, qui indique aux législateurs nationaux des principes directeurs pour définir certaines infractions informatiques, ainsi que la Recommandation n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information;

Eu égard à la Résolution n° 1, adoptée par les Ministres européens de la Justice à leur 21e Conférence (Prague, juin 1997) qui recommande au Comité des Ministres de soutenir les activités menées par le Comité européen pour les problèmes criminels (CDPC) concernant la cybercriminalité afin de rapprocher les législations pénales nationales et de permettre l'utilisation de moyens d'investigation efficaces en matière d'infractions informatiques, ainsi qu'à la Résolution N°3, adoptée lors de la 23e Conférence des Ministres européens de la Justice (Londres, juin 2000), qui encourage les parties aux négociations à poursuivre leurs efforts afin de trouver des solutions adaptées permettant au plus grand nombre d'Etats d'être parties à la Convention et reconnaît la nécessité de disposer d'un mécanisme rapide et efficace de coopération internationale qui tienne dûment compte des exigences spécifiques de la lutte contre la cybercriminalité;

Prenant également en compte le Plan d'action adopté par les Chefs d'Etat et de gouvernement du Conseil de l'Europe à l'occasion de leur Deuxième Sommet (Strasbourg, 10 - 11 octobre 1997) afin de chercher des réponses communes au développement des nouvelles technologies

de l'information, fondées sur les normes et les valeurs du Conseil de l'Europe;

Sont convenus de ce qui suit:

Chapitre I - Terminologie

Article 1 – Définitions

Aux fins de la présente Convention, l'expression:

a. «système informatique» désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données;

b. «données informatiques» désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction;

c. «fournisseur de service» désigne :

i. toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ;

ii. toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs ;

d. «données relatives au trafic» désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type du service sous-jacent.

Chapitre II - Mesures à prendre au niveau national

Section 1 - Droit pénal matériel

Titre 1 - Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques

Article 2 - Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 3 - Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y

compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 4 - Atteinte à l'intégrité des données

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

2. Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

Article 5 - Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération et la suppression de données informatiques.

Article 6 – Abus de dispositifs

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:

a. la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition

i. d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 – 5 ci-dessus ;

ii. d'un mot de passe, d'un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique

dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 – 5 ; et

b. la possession d'un élément visé aux paragraphes (a) (1) ou (2) ci-dessus dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 – 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2. Le présent article ne saurait être interpréter comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'a pas pour but de commettre une infraction établie conformément à l'Article 2 à 5 de la présente Convention, comme en cas d'essais autorisés ou de protection d'un système informatique.

3. Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre

mise à disposition des éléments mentionnés au paragraphe 1 (a)(2).

Titre 2 - Infractions informatiques

Article 7 - Falsification informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger en droit interne une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

Article 8 - Fraude informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui par:

a. l'introduction, l'altération, l'effacement ou la suppression de données informatiques,

b. toute forme d'atteinte au fonctionnement d'un système informatique,

dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

Titre 3 - Infractions se rapportant au contenu

Article 9 – Infractions se rapportant à la pornographie enfantine

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit:

a. la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique ;

b. l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique;

c. la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique;

d. le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique;

e. la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques.

2. Aux fins du paragraphe 1 ci-dessus, la «pornographie enfantine» comprend toute matière pornographique représentant de manière visuelle :

a. un mineur se livrant à un comportement sexuellement explicite;

b. une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;

c. des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

3. Aux fins du paragraphe 2 ci-dessus, le terme «mineur» désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans.

4. Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1 (d) et 1 (e) et 2 (b) et 2 (c).

Titre 4 - Infractions liées aux atteintes
à la propriété intellectuelle et aux droits connexes

Article 10 - Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle définie par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de la Convention universelle sur le droit d'auteur révisée à Paris le 24 juillet 1971, de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces Conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de la Convention internationale sur la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion faite à Rome (Convention de Rome), de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations, exécutions et phonogrammes, à l'exception de tout droit moral conféré par ces Conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

3. Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.

Titre 5 – Autres formes de responsabilité et de sanctions

Article 11 - Tentative et complicité

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est

commise intentionnellement en vue de la perpétration d'une des infractions établies en application des Articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des Articles 3 à 5, 7, 8, 9 (1)a et 9(1)c de la présente Convention.

3. Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent Article.

Article 12 – Responsabilité des personnes morales

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour faire en sorte que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, sur les bases suivantes:

a. un pouvoir de représentation de la personne morale;

b. une autorité pour prendre des décisions au nom de la personne morale;

c. une autorité pour exercer un contrôle au sein de la personne morale.

2. Outre les cas déjà prévus au paragraphe 1, chaque Partie adopte les mesures nécessaires pour s'assurer qu'une personne morale puisse être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions visées au paragraphe 1 pour le compte de ladite personne morale par une personne physique agissant sous son autorité.

3. Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative.

4. Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.

Article 13 – Sanctions et mesures

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour faire en sorte que les infractions pénales établies en application des articles 2 - 11 soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté.

2. Chaque Partie veille à ce que les personnes morales tenues pour responsables en application de l'article 12 fassent l'objet de sanctions ou mesures pénales ou non pénales effectives, proportionnées et dissuasives, comprenant des sanctions pécuniaires.

Section 2 – Droit procédural

Titre 1 – Dispositions communes

Article 14 – Portée d'application des mesures du droit de procédure

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.

2. Sauf disposition contraire figurant à l'Article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 :

a. aux infractions pénales établies conformément aux articles 2-11 de la présente Convention ;

b. à toutes autres infractions pénales commises au moyen d'un système informatique ; et

c. à la collecte des preuves électroniques de toute infraction pénale.

3. a. Chaque Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'Article 20 qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'Article 21. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20.

b. Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, n'est pas en mesure d'appliquer les mesures visées aux articles 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services qui

i. est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et

ii. n'emploi pas les réseaux publics de télécommunications et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé,

cette Partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée aux articles 20 et 21.

Article 15 – Conditions et sauvegardes

1. Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966) ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.

2. Lorsque cela est approprié eu égard à la nature du pouvoir ou de la procédure concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

3. Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette Section sur les droits, responsabilités et intérêts légitimes des tiers.

Titre 2 – Conservation rapide de données informatiques stockées

Article 16 – Conservation rapide de données informatiques stockées

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2. Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et protéger l'intégrité desdits données pendant une durée aussi longue que nécessaire, jusqu'à maximum 90 jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 17 – Conservation et divulgation rapides de données relatives au trafic

1. Afin d'assurer la conservation des données relatives au trafic en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour:

a. veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de service aient participé à la transmission de cette communication; et

b. assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité de données relatives au trafic suffisante pour permettre l'identification des fournisseurs de service et de la voie par laquelle la communication a été transmise.

2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Titre 3 – Injonction de produire

Article 18 – Injonction de produire

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :

a. à une personne présente sur son territoire de communiquer les données informatiques

spécifiées, en la possession où sous le contrôle de cette personne, et stockées dans un système informatique ou un support de stockage informatique; et

b. à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services;

2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

3. Aux fins du présent article, l'expression « données relatives aux abonnés » désigne toute information, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de service et qui se rapporte aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:

a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;

b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de service ;

c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de service.

Titre 4 – Perquisition et saisie de données informatiques stockées

Article 19 – Perquisition et saisie de données informatiques stockées

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire :

a. à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; et

b. à un support du stockage informatique permettant de stocker des données informatiques

sur son territoire.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1 (a), et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou un d'un accès d'une façon similaire à l'autre système.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes :

a. saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci ou un support de stockage informatique ;

b. réaliser et conserver une copie de ces données informatiques ;

c. préserver l'intégrité des données informatiques stockées pertinentes ; et

d. rendre inaccessibles ou enlever ces données informatiques du système informatique consulté.

4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.

5. Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15.

Titre 5 – Collecte en temps réel de données informatiques

Article 20 – Collecte en temps réel des données relatives au trafic

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à :

a. collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ;

b. obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à :

i. collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii. prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

2. Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1(a), elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 21 – Interception de données relatives au contenu

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes relativement à un éventail d'infractions graves à définir en droit interne, à :

a. collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire ; et

b. obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à :

i. collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire , ou

ii. prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.

2. Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1(a), elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et15.

Section 3 – Compétence

Article 22 – Compétence

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux Articles 2 – 11 de la présente Convention, lorsque l'infraction est commise:

a. sur son territoire ;

b. à bord d'un navire battant pavillon de cette Partie ;

c. à bord d'un aéronef immatriculé dans cette Partie ;

d. par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.

2. Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou conditions spécifiques, les règles de compétence définies aux paragraphes 1b – 1d du

présent article ou dans une partie quelconque de ces paragraphes.

3. Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1 de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.

4. La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.

5. Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée visée dans la présente Convention, les Parties concernées se concertent, lorsque cela est opportun, afin de décider quelle est celle qui est la mieux à même d'exercer les poursuites.

Chapitre III – Coopération internationale

Section 1 – Principes généraux

Titre 1 – Principes généraux relatifs à la coopération internationale

Article 23 – Principes généraux relatifs à la coopération internationale

Les Parties coopèrent conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible les unes avec les autres, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et données informatiques ou pour recueillir les preuves sous forme électronique d'une infraction pénale.

Titre 2 – Principes relatifs à l'extradition

Article 24 – Extradition

1. a. Le présent article s'applique à l'extradition entre les Parties pour les infractions pénales définies conformément aux articles 2 à 11 de la présente Convention, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère.

b. Lorsqu'il est exigé une peine minimale différente, sur la base d'un traité d'extradition tel qu'applicable entre deux ou plusieurs parties, y compris la Convention européenne d'extradition (STE n° 24), ou d'un arrangement reposant sur des législations uniformes ou réciproques, c'est la peine minimum prévue par ce traité ou cet arrangement qui s'applique.

2. Les infractions pénales décrites au paragraphe 1 du présent article sont considérées comme incluses en tant qu'infractions pouvant donner lieu à extradition dans tout traité d'extradition existant entre ou parmi les Parties. Les Parties s'engagent à inclure de telles infractions comme infractions pouvant donner lieu à extradition dans tout traité d'extradition pouvant être conclu entre ou parmi elles.

3. Lorsqu'une Partie conditionne l'extradition à l'existence d'un traité et reçoit une demande d'extradition d'une autre Partie avec laquelle elle n'a pas conclu de traité d'extradition, elle peut considérer la présente Convention comme fondement juridique pour l'extradition au regard de toute infraction pénale mentionnée au paragraphe 1 du présent article.

4. Les Parties qui ne conditionnent pas l'extradition à l'existence d'un traité reconnaissent les infractions pénales mentionnées au paragraphe 1 du présent article comme des infractions pouvant donner lieu entre elles à l'extradition.

5. L'extradition est soumise aux conditions prévues par le droit interne de la Partie requise ou par les traités d'extradition en vigueur, y compris les motifs pour lesquels la Partie requise peut refuser l'extradition.

6. Si l'extradition pour une infraction pénale mentionnée au paragraphe 1 du présent article est refusée uniquement sur la base de la nationalité de la personne recherchée ou parce que la Partie requise s'estime compétente pour cette infraction, la Partie requise soumet l'affaire, à la demande de la Partie requérante, à ses autorités compétentes aux fins de poursuites, et rendra compte en temps utile de l'issue de l'affaire à la Partie requérante. Les autorités en question prendront leur décision et mèneront l'enquête et la procédure de la même manière que pour toute autre infraction de nature comparable conformément à la législation de cette Partie.

7. a. Chaque Partie communique au Secrétaire général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, le nom et l'adresse de chaque autorité responsable de l'envoi ou de la réception d'une demande d'extradition ou d'arrestation provisoire, en l'absence de traité.

b. Le Secrétaire général du Conseil de l'Europe établit et tient à jour un registre des autorités ainsi désignées par les Parties. Chaque Partie doit veiller en permanence à l'exactitude des données figurant dans le registre.

Titre 3 – Principes généraux relatifs à l'entraide

Article 25 – Principes généraux relatifs à l'entraide

1. Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.

2. Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35.

3. Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris le cryptage si nécessaire), avec confirmation officielle ultérieure si l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.

4. Sauf disposition contraire expressément prévue dans les articles du présent Chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.

5. Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, en relation avec laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne

classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.

Article 26 – Information spontanée

1. Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande formulée par cette Partie au titre du présent chapitre.

2. Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou ne soient utilisées que sous certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.

Titre 4 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

Article 27 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

1. En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions des paragraphes 2 à 9 du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du reste de cet article.

2. a. Chaque Partie désigne une ou plusieurs autorités centrales chargées d'envoyer les demandes d'entraide ou d'y répondre, de les exécuter ou de les transmettre aux autorités compétentes pour leur exécution;

b. les autorités centrales communiquent directement les unes avec les autres;

c. chaque Partie, au moment de la signature ou du dépôt de ses instruments de ratification, d'acceptation, d'approbation ou d'adhésion, communique au Secrétaire Général du Conseil de l'Europe les noms et adresses des autorités désignées en application du présent paragraphe;

d. le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités centrales désignées par les Parties. Chaque Partie veille en permanence à l'exactitude des données figurant dans le registre.

3. Les demandes d'entraide sous le présent article sont exécutées conformément à la procédure spécifiée par la Partie requérante, sauf lorsqu'elle est incompatible avec la législation de la Partie requise.

4. Outre les conditions ou motifs de refus prévus à l'Article 25, paragraphe 4, l'entraide peut être refusée par la Partie requise :

a. si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

b. si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

5. La Partie requise peut surseoir à l'exécution de la demande si cela risquerait de porter préjudice à des enquêtes ou procédures conduites par ses autorités.

6. Avant de refuser ou de différer sa coopération, la Partie requise examine, après avoir le cas échéant consulté la Partie requérante, s'il peut être fait droit à la demande partiellement ou sous réserve des conditions qu'elle juge nécessaires.

7. La Partie requise informe rapidement la Partie requérante de la suite qu'elle entend donner à la demande d'entraide. Elle doit motiver son éventuel refus d'y faire droit ou l'éventuel ajournement de la demande. La Partie requise informe également la Partie requérante de tout motif rendant l'exécution de l'entraide impossible ou étant susceptible de la retarder de manière significative.

8. La Partie requérante peut demander que la Partie requise garde confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre restent confidentiels, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si la Partie requise ne peut faire droit à cette demande de confidentialité, elle doit en informer rapidement la Partie requérante, qui devra alors déterminer si la demande doit néanmoins être exécutée.

9. a. En cas d'urgence, les autorités judiciaires de la Partie requérante peuvent adresser directement à leurs homologues de la Partie requise les demandes d'entraide ou les communications s'y rapportant. Dans de tels cas, copie est adressée simultanément aux autorités centrales de la Partie requise par le biais de l'autorité centrale de la Partie requérante

b. Toute demande ou communication formulée au titre du présent paragraphe peut l'être par l'intermédiaire de l'Organisation internationale de police criminelle (Interpol).

c. Lorsqu'une demande a été formulée en application de l'alinéa (a) du présent article et que l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité nationale compétente et en informe directement la Partie requérante.

d. Les demandes ou communications effectuées en application du présent paragraphe qui ne supposent pas de mesure de coercition peuvent être directement transmises par les autorités compétentes de la Partie requérante aux autorités compétentes de la Partie requise.

e. Chaque Partie peut informer le Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, que, pour des raisons d'efficacité, les demandes faites sous ce paragraphe devront être adressées à son autorité centrale.

Article 28 – Confidentialité et restriction d'utilisation

1. En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du présent article.

2. La Partie requise peut subordonner la communication d'informations ou de matériels en réponse à une demande à la condition :

établies conformément aux articles 2 à 11 de la présente Convention, se réserver le droit de refuser la demande de conservation au titre du présent article dans le cas où elle a des raisons de penser qu'au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie.

5. En outre, une demande de conservation peut être refusée uniquement :

a. si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

a. si la Partie requise estime que le fait d'accéder de la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels.

6. Lorsque la Partie requise estime que la conservation simple ne suffira pas pour garantir la disponibilité future des données, compromettra la confidentialité de l'enquête de la Partie requérante ou nuira d'une autre façon à celle-ci, elle en informe rapidement la Partie requérante, qui décide alors s'il convient néanmoins d'exécuter la demande.

7. Toute conservation effectuée en réponse à une demande visée au paragraphe 1 sera valable pour une période d'au moins 60 jours afin de permettre à la Partie requérante de soumettre une demande en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données. Après la réception d'une telle demande, les données doivent continuer à être conservées en attendant l'adoption d'une décision concernant la demande.

Article 30 – Divulgation rapide de données conservées

1. Lorsqu'en exécutant une demande de conservation de données relatives au trafic concernant une communication spécifique formulée en application de l'article 29, la Partie requise découvre qu'un fournisseur de services dans un autre Etat a participé à la transmission de cette communication, la Partie requise divulgue rapidement à la Partie requérante une quantité suffisante de données concernant le trafic, aux fins d'identifier ce fournisseur de service et la voie par laquelle la communication a été transmise.

2. La divulgation de données relatives au trafic en application du paragraphe 1 peut être refusée seulement :

a. si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

b. si elle considère que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

Titre 2 – Entraide concernant les pouvoirs d'investigation

Article 31 – Entraide concernant l'accès aux données stockées

1. Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, et de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément à l'article 29.

2. La Partie requise satisfait à la demande en appliquant les instruments internationaux, les arrangements et les législations évoqués à l'article 23 et en se conformant aux dispositions

pertinentes du présent chapitre.

3. La demande doit être satisfaite aussi rapidement que possible dans les cas suivants:

a. il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification ; ou

b. les instruments, arrangements et législations évoqués au paragraphe 2 prévoient une coopération rapide.

Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public

Une Partie peut, sans l'autorisation d'une autre Partie, :

a. accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou

b. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

Article 33 – Entraide dans la collecte en temps réel de données relatives au trafic

1. Les Parties s'accordent l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur leur territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions du paragraphe 2, cette entraide est régie par les conditions et procédures prévues en droit interne.

2. Chaque Partie accorde cette entraide au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne.

Article 34 – Entraide en matière d'interception de données relatives au contenu

Les Parties s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables, pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique.

Titre 3 – Réseau 24/7

Article 35 – Réseau 24/7

1. Chaque Partie désigne un point de contact joignable 24 heures sur 24, sept jours sur sept, afin d'assurer la fourniture d'une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et données informatiques ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes :

a. apport de conseils techniques;

b. conservation des données conformément aux articles 29 et 30 ; et

c. recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.

2. a. Le point de contact d'une Partie pourra correspondre avec le point de contact d'une autre Partie selon une procédure accélérée.

b. Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités selon une procédure accélérée.

3. Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.

Chapitre IV – Clauses finales

Article 36 – Signature et entrée en vigueur

1. La présente Convention est ouverte à la signature des Etats membres du Conseil de l'Europe et des Etats non membres qui ont participé à son élaboration.

2. La présente Convention est soumise à ratification, acceptation ou approbation. Les instruments de ratification, d'acceptation ou d'approbation sont déposés auprès du Secrétaire Général du Conseil de l'Europe.

3. La présente Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Etats, incluant au moins trois Etats membres du Conseil de l'Europe, auront exprimé leur consentement à être liés par la Convention, conformément aux dispositions des paragraphes 1 et 2.

4. Pour tout Etat signataire qui exprimera ultérieurement son consentement à être lié par la Convention, celle-ci entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de l'expression de son consentement à être lié par la Convention conformément aux dispositions des paragraphes 1 et 2.

Article 37 – Adhésion à la Convention

1. Après l'entrée en vigueur de la présente Convention, le Comité des Ministres du Conseil de l'Europe peut, après avoir consulté les Etats contractants à la Convention et en avoir obtenu l'assentiment unanime, inviter tout Etat non membre du Conseil et n'ayant pas participé à son élaboration à adhérer à la présente Convention. La décision est prise à la majorité prévue à l'article 20.d du Statut du Conseil de l'Europe et à l'unanimité des représentants des Etats contractants ayant le droit de siéger au Comité des Ministres.

2. Pour tout Etat adhérent à la Convention conformément au paragraphe 1 ci-dessus, la Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de dépôt de l'instrument d'adhésion près le Secrétaire Général du Conseil de l'Europe.

Article 38 – Application territoriale

1. Tout Etat peut, au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, désigner le ou les territoires sur lesquels s'appliquera la présente Convention.

2. Tout Etat peut, à tout autre moment par la suite, par déclaration adressée au Secrétaire Général du Conseil de l'Europe, étendre l'application de la présente Convention à tout autre territoire désigné dans la déclaration. La Convention entrera en vigueur à l'égard de ce territoire le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la déclaration par le Secrétaire Général.

3. Toute déclaration faite en application des deux paragraphes précédents peut être retirée, en ce qui concerne tout territoire désigné dans cette déclaration, par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de ladite notification par le Secrétaire Général.

Article 39 – Effets de la Convention

1. L'objet de la présente Convention est de compléter les traités ou accords multilatéraux ou bilatéraux applicables existant entre les Parties, y compris les dispositions:

- de la Convention européenne d'extradition ouverte à la signature le 13 décembre 1957 à Paris [STE n°24];

- de la Convention européenne d'entraide judiciaire en matière pénale ouverte à la signature le 20 avril 1959 à Strasbourg [STE n°30];

- du Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale ouvert à la signature le 17 mars 1978 à Strasbourg [STE n°99].

2. Si deux ou plusieurs Parties ont déjà conclu un accord ou un traité relatif aux matières traitées par la présente Convention ou si elles ont autrement établi leurs relations sur ces sujets, ou si elles le feront à l'avenir, elles ont aussi la faculté d'appliquer ledit accord ou traité ou d'établir leurs relations en conséquence, au lieu de la présente Convention. Toutefois, lorsque les Parties établiront leurs relations concernant les matières faisant l'objet de la présente Convention d'une manière différente de celle y prévue, elles le feront d'une manière qui ne soit pas incompatible avec les objectifs et principes de la Convention.

3. Rien dans la présente Convention n'affecte d'autres droits, restrictions, obligations et responsabilités d'une Partie.

Article 40 – Déclarations

Par déclaration écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la faculté d'exiger, le cas échéant, un ou plusieurs éléments supplémentaires tels que prévus aux Articles 2, 3, 6, paragraphe 1(b), 7, 9, paragraphe 3 et 27, paragraphe 9(e).

Article 41 – Clause fédérale

1. Un État fédéral peut se réserver le droit d'honorer les obligations aux termes du Chapitre II de la présente Convention dans la mesure où celles-ci sont compatibles avec les principes fondamentaux qui gouvernent les relations entre son gouvernement central et les États constituants ou autres entités territoriales analogues, à condition qu'il soit en mesure de coopérer sur la base du Chapitre III.

2. Lorsqu'il fait une réserve prévue au paragraphe 1, un État [illegible] faire usage des

termes d'une telle réserve pour exclure ou diminuer de manière substantielle ses obligations en vertu du chapitre II. En tout état de cause, il se dote de moyens étendus et effectifs permettant la mise en oeuvre des mesures prévues par ledit chapitre.

3. En ce qui concerne les dispositions de cette Convention dont l'application relève de la compétence législative de chacun des Etats constituants ou autres entités territoriales analogues, qui ne sont pas, en vertu du système constitutionnel de la fédération, tenus de prendre des mesures législatives, le gouvernement fédéral porte, avec son avis favorable, lesdites dispositions à la connaissance des autorités compétentes des Etats constituants, en les encourageant à adopter les mesures appropriées pour les mettre en oeuvre.

Article 42 – Réserves

Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la ou les réserves prévues aux Article 4, paragraphe 2, Article 6, paragraphe 3, Article 9, paragraphe 4, Article 10, paragraphe 3, Article 11, paragraphe 3, Article 14, paragraphe 3, Article 22, paragraphe 2, Article 29, paragraphe 4, et à l'article 41, paragraphe 1. Aucune autre réserve ne peut être faite.

Article 43 – Statut et retrait des réserves

1. Une Partie qui a fait une réserve conformément à l'Article 42 peut la retirer en totalité ou en partie par notification adressée au Secrétaire Général. Ce retrait prend effet à la date de réception de ladite notification par le Secrétaire Général. Si la notification indique que le retrait d'une réserve doit prendre effet à une date précise, et si cette date est postérieure à celle à laquelle le Secrétaire Général reçoit la notification, le retrait prend effet à cette date ultérieure.

2. Une Partie qui a fait une réserve comme celles mentionnées à l'Article 42 retire cette réserve, en totalité ou en partie, dès que les circonstances le permettent.

3. Le Secrétaire Général du Conseil de l'Europe peut périodiquement demander aux Parties ayant fait une ou plusieurs réserves comme celles mentionnées à l'Article 42 des informations, sur les perspectives de leur retrait.

Article 44 – Amendements

1. Des amendements à la présente Convention peuvent être proposés par chaque Partie, et sont communiqués par le Secrétaire Général du Conseil de l'Europe aux États membres du Conseil de l'Europe, aux États non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout État y ayant adhéré ou ayant été invité à y adhérer conformément aux dispositions de l'article 37.

2. Tout amendement proposé par une Partie est communiqué au Comité européen pour les problèmes criminels (CDPC), qui soumet au Comité des Ministres son avis sur ledit amendement.

3. Le Comité des Ministres examine l'amendement proposé et l'avis soumis par le Comité européen pour les problèmes criminels (CDPC) et, après consultation avec les Etats non membres parties à la présente Convention, peut adopter l'amendement.

4. Le texte de tout amendement adopté par le Comité des Ministres conformément au paragraphe 3 du présent article est communiqué aux Parties pour acceptation.

5. Tout amendement adopté conformément au paragraphe 3 du présent article entre en vigueur le trentième jour après que toutes les Parties ont informé le Secrétaire Général de leur acceptation.

Article 45 – Règlement des différends

1. Le Comité européen pour les problèmes criminels du Conseil de l'Europe est tenu informé de l'interprétation et de l'application de la présente Convention.

2. En cas de différend entre les Parties sur l'interprétation ou l'application de la présente Convention, les Parties s'efforceront de parvenir à un règlement du différend par la négociation ou par tout autre moyen pacifique de leur choix, y compris la soumission du différend au Comité européen pour les problèmes criminels, à un tribunal arbitral qui prendra des décisions qui lieront les Parties au différend, ou à la Cour internationale de justice, selon un accord commun entre les Parties concernées.

Article 46 – Concertation des Parties

1. Les Parties se concertent périodiquement, au besoin, afin de faciliter :

a. l'usage et la mise en œuvre effectifs de la présente Convention, y compris l'identification de tout problème en la matière, ainsi que les effets de toute déclaration ou réserve faite conformément à la présente Convention;

b. l'échange d'informations sur les nouveautés juridiques, politiques ou techniques importantes observées dans le domaine de la criminalité informatique et la collecte de preuves sous forme électronique ;

c. l'examen de l'éventualité de compléter ou d'amender la Convention.

2. Le Comité européen pour les problèmes criminels (CDPC) est tenu périodiquement au courant du résultat des concertations mentionnées au paragraphe 1.

3. Le Comité européen pour les problèmes criminels (CDPC) facilite, au besoin, les concertations mentionnées au paragraphe 1 et adopte les mesures nécessaires pour aider les Parties dans leurs efforts visant à compléter ou amender la Convention. Au plus tard à l'issue d'un délai de trois ans à compter de l'entrée en vigueur de la présente Convention, le Comité européen pour les problèmes criminels (CDPC) procèdera, en coopération avec les Parties, à un réexamen de l'ensemble des dispositions de la Convention et proposera, le cas échéant, les aménagement appropriés.

4. Sauf lorsque le Conseil de l'Europe les prend en charge, les frais occasionnés par l'application des dispositions du paragraphe 1 sont supportés par les Parties de la manière qu'elles déterminent.

5. Les Parties sont assistées par le Secrétariat du Conseil de l'Europe dans l'exercice de leurs fonctions découlant du présent article.

Article 47 – Dénonciation

1 Toute Partie peut, à tout moment, dénoncer la présente Convention par notification au Secrétaire Général du Conseil de l'Europe.

2 La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une periode de

trois mois après la date de réception de la notification par le Secrétaire Général.

Article 48 – Notification

Le Secrétaire Général du Conseil de l'Europe notifie aux États membres du Conseil de l'Europe, aux États non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout État y ayant adhéré ou ayant été invité à y adhérer :

a. toute signature;

b. le dépôt de tout instrument de ratification, d'acceptation, d'approbation ou d'adhésion;

c. toute date d'entrée en vigueur de la présente Convention conformément à ses articles 36 et 37 ;

d. toute déclaration faite en application des Articles 40 et 41 ou toute réserve faite en application de l'article 42 ;

e. tout autre acte, notification ou communication ayant trait à la présente Convention.

En foi de quoi, les soussignés, dûment autorisés à cet effet, ont signé la présente Convention.

Fait à Budapest, le 23 novembre 2001, en français et en anglais, les deux textes faisant également foi, et en un seul exemplaire qui sera déposé dans les archives du Conseil de l'Europe. Le Secrétaire Général du Conseil de l'Europe en communiquera copie certifiée conforme à chacun des Etats membres du Conseil de l'Europe, aux Etats non membres qui ont participé à l'élaboration de la Convention et à tout Etat invité à y adhérer.

الفهرس

الفهرس :